**微软发布****4月补丁修复****76个安全问题**

**安全威胁通告**



发布时间：2019年4月10日

## 综述

微软于周二发布了4月安全更新补丁，修复了76个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及.NET Core、Adobe Flash Player、CSRSS、Microsoft Browsers、Microsoft Edge、Microsoft Exchange Server、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Office、Microsoft Office SharePoint、Microsoft Scripting Engine、Microsoft Windows、Microsoft XML、Open Source Software、Servicing Stack Updates、Team Foundation Server、Windows Admin Center、Windows Kernel以及Windows SMB Server。

相关信息如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 产品 | CVE 编号 | CVE 标题 | 严重程度 |
| .NET Core | CVE-2019-0815 | ASP.NET Core 拒绝服务漏洞 | Important |
| Adobe Flash Player | ADV190011 | April 2019 Adobe Flash 安全更新 | Critical |
| CSRSS | CVE-2019-0735 | Windows CSRSS 特权提升漏洞 | Important |
| Microsoft Browsers | CVE-2019-0764 | Microsoft Browsers Tampering Vulnerability | Low |
| Microsoft Edge | CVE-2019-0833 | Microsoft Edge 信息泄露漏洞 | Important |
| Microsoft Exchange Server | CVE-2019-0858 | Microsoft Exchange 欺骗漏洞 | Important |
| Microsoft Exchange Server | CVE-2019-0817 | Microsoft Exchange 欺骗漏洞 | Important |
| Microsoft Graphics Component | CVE-2019-0802 | Windows GDI 信息泄露漏洞 | Important |
| Microsoft Graphics Component | CVE-2019-0803 | Win32k 特权提升漏洞 | Important |
| Microsoft Graphics Component | CVE-2019-0849 | Windows GDI 信息泄露漏洞 | Important |
| Microsoft Graphics Component | CVE-2019-0853 | GDI+ 远程代码执行漏洞 | Critical |
| Microsoft JET Database Engine | CVE-2019-0846 | Jet Database Engine 远程代码执行漏洞 | Important |
| Microsoft JET Database Engine | CVE-2019-0847 | Jet Database Engine 远程代码执行漏洞 | Important |
| Microsoft JET Database Engine | CVE-2019-0851 | Jet Database Engine 远程代码执行漏洞 | Important |
| Microsoft JET Database Engine | CVE-2019-0877 | Jet Database Engine 远程代码执行漏洞 | Important |
| Microsoft JET Database Engine | CVE-2019-0879 | Jet Database Engine 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0822 | Microsoft Graphics Components 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0823 | Microsoft Office Access Connectivity Engine 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0824 | Microsoft Office Access Connectivity Engine 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0825 | Microsoft Office Access Connectivity Engine 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0826 | Microsoft Office Access Connectivity Engine 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0827 | Microsoft Office Access Connectivity Engine 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0801 | Office 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2019-0828 | Microsoft Excel 远程代码执行漏洞 | Important |
| Microsoft Office SharePoint | CVE-2019-0830 | Microsoft Office SharePoint XSS Vulnerability | Important |
| Microsoft Office SharePoint | CVE-2019-0831 | Microsoft Office SharePoint XSS Vulnerability | Important |
| Microsoft Scripting Engine | CVE-2019-0739 | Scripting Engine 内存破坏漏洞 | Critical |
| Microsoft Scripting Engine | CVE-2019-0812 | Chakra Scripting Engine 内存破坏漏洞 | Critical |
| Microsoft Scripting Engine | CVE-2019-0829 | Chakra Scripting Engine 内存破坏漏洞 | Critical |
| Microsoft Scripting Engine | CVE-2019-0752 | Scripting Engine 内存破坏漏洞 | Important |
| Microsoft Scripting Engine | CVE-2019-0753 | Scripting Engine 内存破坏漏洞 | Critical |
| Microsoft Scripting Engine | CVE-2019-0806 | Chakra Scripting Engine 内存破坏漏洞 | Critical |
| Microsoft Scripting Engine | CVE-2019-0810 | Chakra Scripting Engine 内存破坏漏洞 | Moderate |
| Microsoft Scripting Engine | CVE-2019-0835 | Microsoft Scripting Engine 信息泄露漏洞 | Important |
| Microsoft Scripting Engine | CVE-2019-0860 | Chakra Scripting Engine 内存破坏漏洞 | Moderate |
| Microsoft Scripting Engine | CVE-2019-0861 | Chakra Scripting Engine 内存破坏漏洞 | Critical |
| Microsoft Scripting Engine | CVE-2019-0862 | Scripting Engine 内存破坏漏洞 | Important |
| Microsoft Windows | CVE-2019-0794 | OLE Automation 远程代码执行漏洞 | Important |
| Microsoft Windows | CVE-2019-0805 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0838 | Windows 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2019-0839 | Windows 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2019-0840 | Windows Kernel 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2019-0841 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0842 | Windows VBScript Engine 远程代码执行漏洞 | Important |
| Microsoft Windows | CVE-2019-0845 | Windows IOleCvt Interface 远程代码执行漏洞 | Critical |
| Microsoft Windows | CVE-2019-0848 | Win32k 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2019-0685 | Win32k 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0688 | Windows TCP/IP 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2019-0730 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0731 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0732 | Windows 安全功能绕过漏洞 | Important |
| Microsoft Windows | CVE-2019-0796 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0814 | Win32k 信息泄露漏洞 | Important |
| Microsoft Windows | CVE-2019-0836 | Windows 特权提升漏洞 | Important |
| Microsoft Windows | CVE-2019-0837 | DirectX 信息泄露漏洞 | Important |
| Microsoft XML | CVE-2019-0790 | MS XML 远程代码执行漏洞 | Critical |
| Microsoft XML | CVE-2019-0791 | MS XML 远程代码执行漏洞 | Critical |
| Microsoft XML | CVE-2019-0792 | MS XML 远程代码执行漏洞 | Critical |
| Microsoft XML | CVE-2019-0793 | MS XML 远程代码执行漏洞 | Critical |
| Microsoft XML | CVE-2019-0795 | MS XML 远程代码执行漏洞 | Critical |
| Open Source Software | CVE-2019-0876 | Open Enclave SDK 信息泄露漏洞 | Important |
| Servicing Stack Updates | ADV990001 | Latest Servicing Stack Updates | Critical |
| Team Foundation Server | CVE-2019-0857 | Azure DevOps Server 欺骗漏洞 | Important |
| Team Foundation Server | CVE-2019-0866 | Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability | Important |
| Team Foundation Server | CVE-2019-0867 | Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability | Important |
| Team Foundation Server | CVE-2019-0868 | Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability | Important |
| Team Foundation Server | CVE-2019-0869 | Azure DevOps Server HTML Injection Vulnerability | Important |
| Team Foundation Server | CVE-2019-0870 | Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability | Important |
| Team Foundation Server | CVE-2019-0871 | Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability | Important |
| Team Foundation Server | CVE-2019-0874 | Azure DevOps Server Cross-site Scripting Vulnerability | Important |
| Team Foundation Server | CVE-2019-0875 | Azure DevOps Server 特权提升漏洞 | Important |
| Windows Admin Center | CVE-2019-0813 | Windows Admin Center 特权提升漏洞 | Important |
| Windows Kernel | CVE-2019-0844 | Windows Kernel 信息泄露漏洞 | Important |
| Windows Kernel | CVE-2019-0856 | Windows 远程代码执行漏洞 | Important |
| Windows Kernel | CVE-2019-0859 | Win32k 特权提升漏洞 | Important |
| Windows SMB Server | CVE-2019-0786 | SMB Server 特权提升漏洞 | Critical |

## 修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

## 附件

# ADV190011 - April 2019 Adobe Flash Security Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV190011 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV190011) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV190011) | **CVE Title:** April 2019 Adobe Flash Security Update  **Description:**  This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin [APSB19-19](http://helpx.adobe.com/security/products/flash-player/apsb19-19.html): CVE-2019-7096, CVE-2019-7108.  **FAQ:**  **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit any of these vulnerabilities. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.  In a web-based attack scenario where the user is using Internet Explorer in the Windows 8-style UI, an attacker would first need to compromise a website already listed in the Compatibility View (CV) list. An attacker could then host a website that contains specially crafted Flash content designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. For more information about Internet Explorer and the CV List, please see the MSDN Article, Developer Guidance for websites with content for Adobe Flash Player in Windows 8.  **Mitigations:**  **Workarounds:**  Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update.  **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry.  **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps:   1. Paste the following into a text file and save it with the .reg file extension. 2. Windows Registry Editor Version 5.00 3. [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 4. "Compatibility Flags"=dword:00000400 5. [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 6. "Compatibility Flags"=dword:00000400 7. Double-click the .reg file to apply it to an individual system.   You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection.  **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround. **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy** **Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites:  [Group Policy Overview](https://technet.microsoft.com/library/hh831791) [What is Group Policy Object Editor?](https://technet.microsoft.com/library/cc737816%28v=ws.10%29.aspx) [Core Group Policy tools and settings](https://technet.microsoft.com/library/cc784165%28v=ws.10%29.aspx)  To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010.   1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to Enabled. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. **Prevent Adobe Flash Player from running in Office 2010 on affected systems** **Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.   To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps:   1. Create a text file named Disable\_Flash.reg with the following contents:   [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]  "Compatibility Flags"=dword:00000400   1. Double-click the .reg file to apply it to an individual system. 2. **Note** You must restart Internet Explorer for your changes to take effect. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, [Group Policy collection](http://go.microsoft.com/fwlink/?LinkID=215719). **Prevent ActiveX controls from running in Office 2007 and Office 2010**   To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps:   1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then select Disable all controls without notifications. 3. Click OK to save your settings. **Impact of workaround**. Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround**.   To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps:   1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then deselect Disable all controls without notifications. 3. Click OK to save your settings. **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High.   To raise the browsing security level in Internet Explorer, perform the following steps:   1. On the Internet Explorer **Tools** menu, click\*\* Internet Option\*\*s. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround**. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone**   You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps:   1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround**. There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.   To do this, perform the following steps:   1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are \***.windowsupdate.microsoft.com** and \***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update.   **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **ADV190011** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Adobe Flash Player on Windows Server 2012 | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for 32-bit systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for x64-based systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2012 R2 | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows RT 8.1 | 4493478 Security Update | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for 32-bit Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for x64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2016 | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1803 for 32-bit Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1803 for x64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1803 for ARM64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1809 for 32-bit Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1809 for x64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1809 for ARM64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2019 | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for ARM64-based Systems | [4493478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493478) | Critical | Remote Code Execution | 4489907 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# ADV990001 - Latest Servicing Stack Updates

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV990001 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV990001) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV990001) | **CVE Title:** Latest Servicing Stack Updates  **Description:**  This is a list of the latest servicing stack updates for each operating sytem. This list will be updated whenever a new servicing stack update is released. It is important to install the latest servicing stack update.  **FAQ:**  **1. Why are all of the Servicing Stack Updates (SSU) critical updates?**  The SSUs are classified as Critical updates. This does not indicate that there is a critical vulnerability being addressed in the update.  **2. When was the most recent SSU released for each version of Microsoft Windows?**  Please refer to the following table for the most recent SSU release. We will update the entries any time a new SSU is released:   | **Product** | **SSU Package** | **Date Released** | | --- | --- | --- | | Windows Server 2008 | 4493730 | April 2019 | | Windows 7/Server 2008 R2 | 4490628 | March 2019 | | Windows Server 2012 | 3173426 | July 2016 | | Windows 8.1/Server 2012 R2 | 3173424 | July 2016 | | Windows 10 | 4093430 | April 2018 | | Windows 10 Version 1607/Server 2016 | 4485447 | February 2019 | | Windows 10 Version 1703 | 4487327 | February 2019 | | Windows 10 1709/Windows Server, version 1709 | 4485448 | February 2019 | | Windows 10 1803/Windows Server, version 1803 | 4485449 | February 2019 | | Windows 10 1809/Server 2019 | 4493510 | April 2019 |   **Mitigations:** None  **Workarounds:** None  **Revision:** 1.1    11/14/2018 08:00:00  Corrected the link to the Windows Server 2008 Servicing Stack Update. This is an informational change only.  2.0    12/05/2018 08:00:00  A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information.  5.2    02/14/2019 08:00:00  In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1803 for x64-based Systems to 4485449. This is an informational change only.  3.1    12/11/2018 08:00:00  Updated supersedence information. This is an informational change only.  7.0    04/09/2019 07:00:00  A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 10 version 1809, Windows Server 2019, and Windows Server 2019 (Server Core installation). See the FAQ section for more information.  5.0    02/12/2019 08:00:00  A Servicing Stack Update has been released for Windows 10 Version 1607, Windows Server 2016, and Windows Server 2016 (Server Core installation); Windows 10 Version 1703; Windows 10 Version 1709 and Windows Server, version 1709 (Server Core Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information.  3.2    12/12/2018 08:00:00  Fixed a typo in the FAQ.  1.2    12/03/2018 08:00:00  FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only.  5.1    02/13/2019 08:00:00  In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1809 for x64-based Systems to 4470788. This is an informational change only.  3.0    12/11/2018 08:00:00  A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information.  4.0    01/08/2019 08:00:00  A Servicing Stack Update has been released for Windows 10 Version 1703. See the FAQ section for more information.  1.0    11/13/2018 08:00:00  Information published.  2.0    12/05/2018 08:00:00  A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information.  6.0    03/12/2019 07:00:00  A Servicing Stack Update has been released for Windows 7 and Windows Server 2008 R2 and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information. | Critical | Defense in Depth |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **ADV990001** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4490628 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4490628) | Critical | Defense in Depth |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4490628 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4490628) | Critical | Defense in Depth |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4490628 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4490628) | Critical | Defense in Depth |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4490628 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4490628) | Critical | Defense in Depth |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4490628 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4490628) | Critical | Defense in Depth |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493730 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493730) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 | [3173426 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3173426) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 (Server Core installation) | [3173426 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3173426) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 8.1 for 32-bit systems | [3173424 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3173424) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 8.1 for x64-based systems | [3173424 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3173424) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 R2 | [3173424 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3173424) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 R2 (Server Core installation) | [3173424 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3173424) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 for 32-bit Systems | [4093430 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093430) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 for x64-based Systems | [4093430 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093430) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2016 | [4485447 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485447) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4485447 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485447) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4485447 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485447) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2016 (Server Core installation) | [4485447 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485447) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4487327 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4487327) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4487327 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4487327) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4485448 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485448) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4485448 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485448) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4485448 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485448) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4485449 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485449) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4485449 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485449) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4485449 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485449) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4485449 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485449) | Critical | Defense in Depth | 4021701 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493510 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493510) | Critical | Defense in Depth | 4470788 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493510 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493510) | Critical | Defense in Depth | 4470788 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493510 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493510) | Critical | Defense in Depth | 4470788 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2019 | [4493510 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493510) | Critical | Defense in Depth | 4470788 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2019 (Server Core installation) | [4493510 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493510) | Critical | Defense in Depth | 4470788 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4485448 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4485448) | Critical | Defense in Depth | 4470788 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493730 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493730) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493730 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493730) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493730 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493730) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493730 Servicing Stack Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493730) | Critical | Defense in Depth | 955430 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2019-0685 - Win32k Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0685 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0685) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0685) | **CVE Title:** Win32k Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how Win32k handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0685** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0688 - Windows TCP/IP Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0688 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0688) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0688) | **CVE Title:** Windows TCP/IP Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  To exploit this vulnerability, an attacker would have to send specially crafted fragmented IP packets to a remote Windows computer. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.  The update addresses the vulnerability by correcting how the Windows TCP/IP stack handles fragmented IP packets.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is device information like resource ids, sas tokens, user properties, and other sensitive information.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0688** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.3 Temporal: 4.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C | Yes |

# CVE-2019-0730 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0730 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0730) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0730) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system.  The update addresses the vulnerability by correcting how Windows handles calls to LUAFV.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0730** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0731 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0731 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0731) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0731) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system.  The update addresses the vulnerability by correcting how Windows handles calls to LUAFV.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0731** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0732 - Windows Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0732 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0732) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0732) | **CVE Title:** Windows Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys). An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.  The update addresses the vulnerability by correcting how Windows validates User Mode Code Integrity policies.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0732** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Security Feature Bypass | 4489878 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Security Feature Bypass | 4489878 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Security Feature Bypass | 4489878 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Security Feature Bypass | 4489878 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Security Feature Bypass | 4489878 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Security Feature Bypass | 4489880 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Security Feature Bypass | 4489891 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Security Feature Bypass | 4489891 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Security Feature Bypass | 4489881 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Security Feature Bypass | 4489881 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Security Feature Bypass | 4489881 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Security Feature Bypass | 4489881 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Security Feature Bypass | 4489881 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Security Feature Bypass | 4489872 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Security Feature Bypass | 4489872 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Security Feature Bypass | 4489882 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Security Feature Bypass | 4489882 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Security Feature Bypass | 4489882 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Security Feature Bypass | 4489882 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Security Feature Bypass | 4489871 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Security Feature Bypass | 4489871 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Security Feature Bypass | 4489886 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Security Feature Bypass | 4489886 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Security Feature Bypass | 4489886 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Security Feature Bypass | 4489868 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Security Feature Bypass | 4489868 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Security Feature Bypass | 4489868 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Security Feature Bypass | 4489868 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Security Feature Bypass | 4489899 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Security Feature Bypass | 4489899 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Security Feature Bypass | 4489899 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Security Feature Bypass | 4489899 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Security Feature Bypass | 4489899 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Security Feature Bypass | 4489886 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Security Feature Bypass | 4489880 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Security Feature Bypass | 4489880 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Security Feature Bypass | 4489880 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Security Feature Bypass | 4489880 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2019-0735 - Windows CSRSS Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0735 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0735) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0735) | **CVE Title:** Windows CSRSS Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system.  The update addresses the vulnerability by correcting how the Windows CSRSS handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0735** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0739 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0739 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0739) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0739) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0739** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Maybe |

# CVE-2019-0752 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0752 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0752) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0752) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0752** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Remote Code Execution | 4489873 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Remote Code Execution | 4489873 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Low | Remote Code Execution | 4489882 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Low | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Remote Code Execution | 4489873 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0753 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0753 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0753) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0753) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0753** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Critical | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Critical | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Moderate | Remote Code Execution | 4489873 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Critical | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Critical | Remote Code Execution | 4489873 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Moderate | Remote Code Execution | 4489873 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Moderate | Remote Code Execution | 4489873 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0764 - Microsoft Browsers Tampering Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0764 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0764) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0764) | **CVE Title:** Microsoft Browsers Tampering Vulnerability  **Description:**  A tampering vulnerability exists when Microsoft browsers do not properly validate input under specific conditions. An attacker who exploited the vulnerability could pass custom command line parameters.  In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message.  The security update addresses the vulnerability by correcting how Microsoft browsers validate input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Low | Tampering |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0764** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Low | Tampering | 4489880 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Low | Tampering | 4489880 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Tampering | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Tampering | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Tampering | 4489873 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Tampering | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Tampering | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Tampering | 4489873 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4493446 Monthly Rollup | Important | Tampering | 4489881 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Tampering | 4489872 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Tampering | 4489872 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Low | Tampering | 4489882 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Tampering | 4489882 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Tampering | 4489882 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Tampering | 4489871 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Tampering | 4489871 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Tampering | 4489886 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Tampering | 4489886 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Tampering | 4489868 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Tampering | 4489868 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Tampering | 4489868 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Tampering | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Tampering | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Tampering | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Low | Tampering | 4489899 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Tampering | 4489886 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Tampering | 4489873 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Tampering | 4489872 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Tampering | 4489872 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Low | Tampering | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Tampering | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Tampering | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Tampering | 4489871 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Tampering | 4489871 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Tampering | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Tampering | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Tampering | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Tampering | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Tampering | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Tampering | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Tampering | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Tampering | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Low | Tampering | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Tampering | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2019-0786 - SMB Server Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0786 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0786) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0786) | **CVE Title:** SMB Server Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine. An attacker who successfully exploited this vulnerability could bypass certain security checks in the operating system.  To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses the vulnerability by correcting how Windows SMB Server handles such specially crafted files.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0786** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0790 - MS XML Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0790 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0790) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0790) | **CVE Title:** MS XML Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system.  To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system.  The update addresses the vulnerability by correcting how the MSXML parser processes user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0790** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0791 - MS XML Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0791 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0791) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0791) | **CVE Title:** MS XML Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system.  To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system.  The update addresses the vulnerability by correcting how the MSXML parser processes user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0791** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0792 - MS XML Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0792 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0792) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0792) | **CVE Title:** MS XML Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system.  To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system.  The update addresses the vulnerability by correcting how the MSXML parser processes user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0792** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0793 - MS XML Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0793 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0793) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0793) | **CVE Title:** MS XML Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system.  To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system.  The update addresses the vulnerability by correcting how the MSXML parser processes user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0793** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0794 - OLE Automation Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0794 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0794) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0794) | **CVE Title:** OLE Automation Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when OLE automation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could gain execution on the victim system.  To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke OLE automation through a web browser. However, an attacker would have to entice a user to visit such a website.  The update addresses the vulnerability by correcting how OLE automation handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0794** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0795 - MS XML Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0795 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0795) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0795) | **CVE Title:** MS XML Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system.  To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system.  The update addresses the vulnerability by correcting how the MSXML parser processes user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0795** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0796 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0796 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0796) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0796) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys). An attacker who successfully exploited this vulnerability could set the short name of a file with a long name to an arbitrary short name, overriding the file system with limited privileges.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability.  The update addresses the vulnerability by correcting how Windows handles calls to LUAFV.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0796** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.3 Temporal: 5.7 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0801 - Office Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0801 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0801) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0801) | **CVE Title:** Office Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when Microsoft Office fails to properly handle certain files.  To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted URL file that points to an Excel or PowerPoint file that was also downloaded.  The update addresses the vulnerability by correcting how Office handles these files.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0801** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4462223 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ae3c90b4-c603-4e86-8142-b4623d3daa56) | Important | Remote Code Execution | 4462174 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4462223 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=425b4af2-686f-4c21-b394-9d5470af739d) | Important | Remote Code Execution | 4462174 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4464504 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d84a593d-83d5-47d2-9c0b-e575562cdc10) | Important | Remote Code Execution | 4462138 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4464504 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b9bb977e-9bb1-4f27-8a88-e441bff6aa1f) | Important | Remote Code Execution | 4462138 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4464504 Security Update | Important | Remote Code Execution | 4462138 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4462242 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b0a43be8-5798-4d1c-b15b-02aadefc0c22) | Important | Remote Code Execution | 4462146 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4462242 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=45529b1e-40bd-4219-adfa-fea835995d10) | Important | Remote Code Execution | 4462146 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4462146 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4462146 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4462146 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4462146 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0802 - Windows GDI Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0802 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0802) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0802) | **CVE Title:** Windows GDI Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.  The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0802** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0803 - Win32k Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0803 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0803) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0803) | **CVE Title:** Win32k Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how Win32k handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0803** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0805 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0805 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0805) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0805) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system.  The update addresses the vulnerability by correcting how Windows handles calls to LUAFV.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0805** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0806 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0806 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0806) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0806) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0806** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Maybe |

# CVE-2019-0810 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0810 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0810) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0810) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0810** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Maybe |

# CVE-2019-0812 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0812 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0812) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0812) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0812** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Maybe |

# CVE-2019-0813 - Windows Admin Center Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0813 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0813) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0813) | **CVE Title:** Windows Admin Center Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows Admin Center improperly impersonates operations in certain situations. An attacker who successfully exploited this vulnerability could gain elevated privileges.  An attacker with unprivileged access to a vulnerable system could exploit this vulnerability.  The security update addresses the vulnerability by ensuring Windows Admin Center properly impersonates operations.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0813** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Admin Center | [4493552 Security Update](https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center) | Important | Elevation of Privilege |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0814 - Win32k Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0814 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0814) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0814) | **CVE Title:** Win32k Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how win32k handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is device information like resource ids, sas tokens, user properties, and other sensitive information.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0814** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0815 - ASP.NET Core Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0815 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0815) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0815) | **CVE Title:** ASP.NET Core Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication.  A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Core application.  The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0815** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ASP.NET Core 2.2 | [Release Notes Security Update](https://dotnet.microsoft.com/download/dotnet-core/2.2) | Important | Denial of Service |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0817 - Microsoft Exchange Spoofing Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0817 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0817) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0817) | **CVE Title:** Microsoft Exchange Spoofing Vulnerability  **Description:**  A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited the vulnerability could perform script or content injection attacks, and attempt to trick the user into disclosing sensitive information. An attacker could also redirect the user to a malicious website that could spoof content or the vulnerability could be used as a pivot to chain an attack with other vulnerabilities in web services.  To exploit the vulnerability, an attacker could send a specially crafted email containing a malicious link to a user. An attacker could also use a chat client to social engineer a user into clicking the malicious link. However, in both examples the user must click the malicious link.  The security update addresses the vulnerability by correcting how OWA validates web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0817** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2010 Service Pack 3 | [4491413 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3adaa6ca-a52c-4a28-8b1d-ea1196073fea) | Important | Spoofing | 4480752 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2019 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=05971399-0bb8-4ede-9b7d-3be188c5ddb7) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 11 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=74a2878b-6978-4f3a-b1f6-bc202195fb01) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 22 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=cdfdbe8a-01ac-412d-a4a7-ecda5bb5dd35) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 12 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=12a706c6-6483-4948-b5a0-06ad02bd7908) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2019 Cumulative Update 1 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9290c8bb-4db5-462e-9b0a-71c992dde85d) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0822 - Microsoft Graphics Components Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0822 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0822) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0822) | **CVE Title:** Microsoft Graphics Components Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system.  To exploit the vulnerability, a user would have to open a specially crafted file.  The security update addresses the vulnerability by correcting how Microsoft Graphics Components handle objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Are the updates for the Microsoft Office for Mac currently available?**  The security update for Microsoft Office 2016 for Mac and Microsoft Office 2019 for Mac are not immediately available. The updates will be released as soon as possible, and when they are available, customers will be notified via a revision to this CVE information.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0822** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2016 for Mac |  | Important | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for Mac |  | Important | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0823 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0823 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0823) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0823) | **CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0823** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c50d78a0-bc94-48a4-91bd-c4d5916c1708) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=34e44967-eb70-45a2-8695-bd63c0f60362) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0824 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0824 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0824) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0824) | **CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0824** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c50d78a0-bc94-48a4-91bd-c4d5916c1708) | Important | Elevation of Privilege | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=34e44967-eb70-45a2-8695-bd63c0f60362) | Important | Elevation of Privilege | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4462204 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=fb5ed147-d01f-40f0-8dad-689d45d3a1c5) | Important | Elevation of Privilege | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4462204 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ebf52bde-972d-4a49-aad5-250eaa52d656) | Important | Elevation of Privilege | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4462204 Security Update | Important | Elevation of Privilege | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1d5c6221-e4d8-4cf3-9d91-7fe8da0f0994) | Important | Elevation of Privilege | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=19352c25-ea16-40d3-b015-c5e7e0a1cff4) | Important | Elevation of Privilege | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Elevation of Privilege | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Elevation of Privilege | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Elevation of Privilege | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Elevation of Privilege | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0825 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0825 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0825) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0825) | **CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0825** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c50d78a0-bc94-48a4-91bd-c4d5916c1708) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=34e44967-eb70-45a2-8695-bd63c0f60362) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1d5c6221-e4d8-4cf3-9d91-7fe8da0f0994) | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=19352c25-ea16-40d3-b015-c5e7e0a1cff4) | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0826 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0826 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0826) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0826) | **CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0826** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c50d78a0-bc94-48a4-91bd-c4d5916c1708) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=34e44967-eb70-45a2-8695-bd63c0f60362) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4462204 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=fb5ed147-d01f-40f0-8dad-689d45d3a1c5) | Important | Remote Code Execution | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4462204 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ebf52bde-972d-4a49-aad5-250eaa52d656) | Important | Remote Code Execution | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4462204 Security Update | Important | Remote Code Execution | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1d5c6221-e4d8-4cf3-9d91-7fe8da0f0994) | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=19352c25-ea16-40d3-b015-c5e7e0a1cff4) | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0827 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0827 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0827) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0827) | **CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0827** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c50d78a0-bc94-48a4-91bd-c4d5916c1708) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4464520 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=34e44967-eb70-45a2-8695-bd63c0f60362) | Important | Remote Code Execution | 4462226 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4462204 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=fb5ed147-d01f-40f0-8dad-689d45d3a1c5) | Important | Remote Code Execution | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4462204 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ebf52bde-972d-4a49-aad5-250eaa52d656) | Important | Remote Code Execution | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4462204 Security Update | Important | Remote Code Execution | 4018300 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1d5c6221-e4d8-4cf3-9d91-7fe8da0f0994) | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4462213 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=19352c25-ea16-40d3-b015-c5e7e0a1cff4) | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4018294 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0828 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0828 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0828) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0828) | **CVE Title:** Microsoft Excel Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.  The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Are the updates for the Microsoft Office for Mac currently available?**  The security update for Microsoft Office 2016 for Mac and Microsoft Office 2019 for Mac are not immediately available. The updates will be released as soon as possible, and when they are available, customers will be notified via a revision to this CVE information.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0828** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4462230 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=a4560532-2795-4e29-bb78-3e6a4ffd68e0) | Important | Remote Code Execution | 4462186 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4462230 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f70bce54-7d8e-46c1-9845-ead72b2ba38e) | Important | Remote Code Execution | 4462186 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | [4462209 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4ac40f0a-5543-4342-855b-b079d1713975) | Important | Remote Code Execution | 4461597 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | [4462209 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c2787cef-d8e8-49cc-a920-bf9307ab805a) | Important | Remote Code Execution | 4461597 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4462209 Security Update | Important | Remote Code Execution | 4461597 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac |  | Important | Remote Code Execution | 4461597 | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft Excel 2016 (32-bit edition) | [4462236 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c98e37e8-6251-428a-b352-3e28d1d33311) | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | [4462236 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9dbfff49-e213-45f2-b154-6adde11fd492) | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2019 for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2019 for Mac |  | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A |  |
| Office 365 ProPlus for 32-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A | No |
| Office 365 ProPlus for 64-bit Systems | Click to Run Security Update | Important | Remote Code Execution | 4462115 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2019-0829 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0829 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0829) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0829) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0829** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0830 - Microsoft Office SharePoint XSS Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0830 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0830) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0830) | **CVE Title:** Microsoft Office SharePoint XSS Vulnerability  **Description:**  A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0830** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Foundation 2013 Service Pack 1 | [4464515 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c3ccd934-34cf-4171-8269-b4f0b0e3e695) | Important | Spoofing | 4462208 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4464510 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=651f7b7b-0ffd-4f87-8220-abecb26b33e6) | Important | Spoofing | 4462211 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Server 2019 | [4464518 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=e9a9e875-9e19-42b1-8726-7c8047693f89) | Important | Spoofing | 4462199 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0831 - Microsoft Office SharePoint XSS Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0831 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0831) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0831) | **CVE Title:** Microsoft Office SharePoint XSS Vulnerability  **Description:**  A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:**  **Is the Preview Pane an attack vector for this vulnerability?**  No, the Preview Pane is not an attack vector.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0831** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Server 2010 Service Pack 2 | [4464525 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c4cb2e8a-2142-4976-9b05-9039af6971fe) | Important | Spoofing | 4462184 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Foundation 2010 Service Pack 2 | [4464528 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4ac767aa-15b0-48d0-891d-ac0fbb0c65df) | Important | Spoofing | 4461630 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4464510 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=651f7b7b-0ffd-4f87-8220-abecb26b33e6) | Important | Spoofing | 4462211 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4464511 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=48dcda63-c7ab-4abc-8c93-2aece103d984) | Important | Spoofing | 4462202 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Server 2019 | [4464518 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=e9a9e875-9e19-42b1-8726-7c8047693f89) | Important | Spoofing | 4462199 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0833 - Microsoft Edge Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0833 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0833) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0833) | **CVE Title:** Microsoft Edge Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0833** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Low | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0835 - Microsoft Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0835 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0835) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0835) | **CVE Title:** Microsoft Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by changing how the scripting engine handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0835** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Low | Information Disclosure | 4489882 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Low | Information Disclosure | 4489899 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Information Disclosure | 4489873 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0836 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0836 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0836) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0836) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control over an affected system.  The update addresses the vulnerability by correcting how Windows handles calls to LUAFV.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0836** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0837 - DirectX Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0837 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0837) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0837) | **CVE Title:** DirectX Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when DirectX improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  An authenticated attacker could exploit this vulnerability by running a specially crafted application.  The update addresses the vulnerability by correcting how DirectX handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0837** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0838 - Windows Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0838 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0838) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0838) | **CVE Title:** Windows Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Â  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability. Â  The security update addresses the vulnerability by changing how Task Scheduler handles credentials.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0838** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2019-0839 - Windows Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0839 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0839) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0839) | **CVE Title:** Windows Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise a userâ€™s system.  To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The update addresses the vulnerability by correcting how the Terminal Services component handle objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0839** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0840 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0840 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0840) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0840) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.  The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0840** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0841 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0841 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0841) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0841) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The security update addresses the vulnerability by correcting how Windows AppX Deployment Service handles hard links.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0841** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0842 - Windows VBScript Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0842 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0842) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0842) | **CVE Title:** Windows VBScript Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0842** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0844 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0844 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0844) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0844) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.  The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0844** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0845 - Windows IOleCvt Interface Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0845 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0845) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0845) | **CVE Title:** Windows IOleCvt Interface Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system.  In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The update addresses the vulnerability by correcting methods exposed when the IOleCvt interface is invoked.  **FAQ:**  **What is IOleCvt interface?**  The Automation interface for the IOleCvt object enables an ASP Web page to perform a variety of string conversions from one format to another. These include:   * Conversion from Unicode to ANSI * Conversion from ANSI to Unicode * Conversion from Unicode to UTF-8 (UCS Transformation Format 8) * Conversion from Unicode using one code page to Unicode using another code page   Although most applications now use Unicode (UTF-16) encoding for character data, some Windows desktop applications use character sets based on Windows code pages. A code page assigns international characters to ANSI character codes greater than 127. For more information, please see [IOleCvt Automation Interface](https://docs.microsoft.com/en-us/windows-hardware/drivers/print/iolecvt-automation-interface).  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0845** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Critical | Remote Code Execution | 4489878 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0846 - Jet Database Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0846 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0846) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0846) | **CVE Title:** Jet Database Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.  **FAQ:**  **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0846** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0847 - Jet Database Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0847 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0847) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0847) | **CVE Title:** Jet Database Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.  **FAQ:**  **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0847** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0848 - Win32k Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0848 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0848) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0848) | **CVE Title:** Win32k Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how win32k handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0848** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0849 - Windows GDI Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0849 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0849) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0849) | **CVE Title:** Windows GDI Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.  The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0849** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2019-0851 - Jet Database Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0851 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0851) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0851) | **CVE Title:** Jet Database Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.  **FAQ:**  **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0851** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Information Disclosure | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Information Disclosure | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Information Disclosure | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Information Disclosure | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Information Disclosure | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Information Disclosure | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Information Disclosure | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Information Disclosure | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Information Disclosure | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Information Disclosure | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Information Disclosure | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Information Disclosure | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Information Disclosure | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0853 - GDI+ Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0853 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0853) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0853) | **CVE Title:** GDI+ Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit the vulnerability:   * In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message. * In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file.   The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0853** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Critical | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Critical | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Critical | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Critical | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | Yes |

# CVE-2019-0856 - Windows Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0856 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0856) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0856) | **CVE Title:** Windows Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could take control of an affected system.  To exploit the vulnerability, an authenticated attacker could connect via the Windows Remote Registry Service, causing Windows to execute arbitrary code.  The security update addresses the vulnerability by correcting how Windows handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published.  1.1    04/09/2019 07:00:00  Corrected vulnerability description and updated one or more CVSS scores for the affected products. These are informational changes only. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0856** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0857 - Azure DevOps Server Spoofing Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0857 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0857) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0857) | **CVE Title:** Azure DevOps Server Spoofing Vulnerability  **Description:**  A spoofing vulnerability that could allow a security feature bypass exists in when Azure DevOps Server does not properly sanitize user provided input. An attacker who exploited the vulnerability could trick a user into loading a page containing malicious content.  An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to the Azure DevOps Server, which would get executed in the context of the user every time a user visits the compromised page. To exploit the bypass, an attacker can leverage any external source in the script-src to embed malicious script by bypassing Content Security Policy (CSP).  The security update addresses the vulnerability by ensuring that Azure DevOps Server sanitizes user input and enforces a strict CSP policy.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0857** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0858 - Microsoft Exchange Spoofing Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0858 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0858) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0858) | **CVE Title:** Microsoft Exchange Spoofing Vulnerability  **Description:**  A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited the vulnerability could perform script or content injection attacks, and attempt to trick the user into disclosing sensitive information. An attacker could also redirect the user to a malicious website that could spoof content or the vulnerability could be used as a pivot to chain an attack with other vulnerabilities in web services.  To exploit the vulnerability, an attacker could send a specially crafted email containing a malicious link to a user. An attacker could also use a chat client to social engineer a user into clicking the malicious link. However, in both examples the user must click the malicious link.  The security update addresses the vulnerability by correcting how OWA validates web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0858** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2019 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=05971399-0bb8-4ede-9b7d-3be188c5ddb7) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 11 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=74a2878b-6978-4f3a-b1f6-bc202195fb01) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 22 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=cdfdbe8a-01ac-412d-a4a7-ecda5bb5dd35) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 12 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=12a706c6-6483-4948-b5a0-06ad02bd7908) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2019 Cumulative Update 1 | [4487563 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9290c8bb-4db5-462e-9b0a-71c992dde85d) | Important | Spoofing | 4471389 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0859 - Win32k Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0859 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0859) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0859) | **CVE Title:** Win32k Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how Win32k handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0859** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Elevation of Privilege | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Elevation of Privilege | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Elevation of Privilege | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Elevation of Privilege | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Elevation of Privilege | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Elevation of Privilege | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Elevation of Privilege | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Elevation of Privilege | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Elevation of Privilege | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Elevation of Privilege | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Elevation of Privilege | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Elevation of Privilege | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Elevation of Privilege | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0860 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0860 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0860) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0860) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0860** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Maybe |

# CVE-2019-0861 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0861 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0861) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0861) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0861** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Critical | Remote Code Execution | 4489872 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Moderate | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Critical | Remote Code Execution | 4489882 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Critical | Remote Code Execution | 4489871 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Critical | Remote Code Execution | 4489868 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Critical | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Moderate | Remote Code Execution | 4489899 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Release Notes Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.11.8) | Critical | Remote Code Execution | 4489886 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Maybe |

# CVE-2019-0862 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0862 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0862) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0862) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0862** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Important | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Low | Remote Code Execution | 4489882 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Low | Remote Code Execution | 4489899 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) [4493435 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493435) | Low | Remote Code Execution | 4489873 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2019-0866 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0866 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0866) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0866) | **CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability  **Description:**  A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.  The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0866** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Team Foundation Server 2017 Update 3.1 | [Release Notes Security Update](https://aka.ms/tfs2017.3.1patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Updated 1.2 | [Release Notes Security Update](https://aka.ms/tfs2018.1.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Update 3.2 | [Release Notes Security Update](https://aka.ms/tfs2018.3.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2015 Update 4.2 | [Release Notes Security Update](https://go.microsoft.com/fwlink/?linkid=844069) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0867 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0867 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0867) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0867) | **CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability  **Description:**  A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.  The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0867** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Team Foundation Server 2018 Update 3.2 | [Release Notes Security Update](https://aka.ms/tfs2018.3.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0868 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0868 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0868) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0868) | **CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability  **Description:**  A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.  The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0868** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Team Foundation Server 2017 Update 3.1 | [Release Notes Security Update](https://aka.ms/tfs2017.3.1patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Updated 1.2 | [Release Notes Security Update](https://aka.ms/tfs2018.1.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Update 3.2 | [Release Notes Security Update](https://aka.ms/tfs2018.3.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0869 - Azure DevOps Server HTML Injection Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0869 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0869) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0869) | **CVE Title:** Azure DevOps Server HTML Injection Vulnerability  **Description:**  A spoofing vulnerability exists in Microsoft Azure DevOps Server when it fails to properly handle web requests. An attacker who successfully exploited the vulnerability could perform script or content injection attacks, and attempt to trick the user into disclosing sensitive information. An attacker could also redirect the user to a malicious website that could spoof content or the vulnerability could be used as a pivot to chain an attack with other vulnerabilities in web services.  To exploit the vulnerability, an attacker could create a popup to harvest information or present a user with a malicious link.  The security update addresses the vulnerability by ensuring that Azure DevOps Server sanitizes user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0869** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0870 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0870 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0870) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0870) | **CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability  **Description:**  A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.  The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0870** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Team Foundation Server 2017 Update 3.1 | [Release Notes Security Update](https://aka.ms/tfs2017.3.1patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Updated 1.2 | [Release Notes Security Update](https://aka.ms/tfs2018.1.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Update 3.2 | [Release Notes Security Update](https://aka.ms/tfs2018.3.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0871 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0871 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0871) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0871) | **CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability  **Description:**  A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.  The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0871** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Team Foundation Server 2017 Update 3.1 | [Release Notes Security Update](https://aka.ms/tfs2017.3.1patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Updated 1.2 | [Release Notes Security Update](https://aka.ms/tfs2018.1.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Team Foundation Server 2018 Update 3.2 | [Release Notes Security Update](https://aka.ms/tfs2018.3.2patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0874 - Azure DevOps Server Cross-site Scripting Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0874 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0874) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0874) | **CVE Title:** Azure DevOps Server Cross-site Scripting Vulnerability  **Description:**  A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server does not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to the Team Foundation Server, which will get executed in the context of the user every time a user visits the compromised page.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content.  The security update addresses the vulnerability by ensuring that Azure DevOps Server sanitizes user inputs.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Spoofing |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0874** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Spoofing |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0875 - Azure DevOps Server Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0875 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0875) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0875) | **CVE Title:** Azure DevOps Server Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Azure DevOps Server 2019 does not properly enforce project permissions. An attacker who exploited the vulnerabilty could add GitHub repos to a project without having the proper access granted to their account.  To exploit the vulnerability, an attacker with access to a project would need to send a specially crafted request to an affected Azure DevOps Server.  The update addresses the vulnerability by correcting the way Azure DevOps Server handles project permissions.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0875** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Azure DevOps Server 2019 | [Release Notes Security Update](https://aka.ms/azdev2019patch) | Important | Elevation of Privilege |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0876 - Open Enclave SDK Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0876 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0876) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0876) | **CVE Title:** Open Enclave SDK Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information stored in the Enclave.  To exploit this vulnerability, an attacker would have to successfully compromise the host application running the enclave. The attacker can then pivot to the enclave and exploit this vulnerability without user interaction.  The security update addresses the vulnerability by modifying how Open Enclave SDK handle objects in memory.  **FAQ:**  **What type of information could be disclosed by this vulnerability?**  The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Enclave memory read - unprivileged write to enclave memory from a host application, which can leak memory contents of the enclave.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0876** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Open Enclave SDK | [Release Notes Security Update](https://github.com/Microsoft/openenclave/commit/d07769bcf73bb8a1b29374be1a50f93bae549f58) | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2019-0877 - Jet Database Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0877 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0877) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0877) | **CVE Title:** Jet Database Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.  **FAQ:**  **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0877** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2019-0879 - Jet Database Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2019-0879 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0879) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0879) | **CVE Title:** Jet Database Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system.  An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file.  The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory.  **FAQ:**  **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/09/2019 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2019-0879** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4493448 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493448) [4493472 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493472) | Important | Remote Code Execution | 4489878 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4493450 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493450) [4493451 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493451) | Important | Remote Code Execution | 4489891 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4493446 Monthly Rollup | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4493446 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493446) [4493467 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493467) | Important | Remote Code Execution | 4489881 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4493475 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493475) | Important | Remote Code Execution | 4489872 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4493470 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493470) | Important | Remote Code Execution | 4489882 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4493474 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493474) | Important | Remote Code Execution | 4489871 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for ARM64-based Systems | [4493464 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493464) | Important | Remote Code Execution | 4489868 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for 32-bit Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for x64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1809 for ARM64-based Systems | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2019 (Server Core installation) | [4493509 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493509) | Important | Remote Code Execution | 4489899 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for ARM64-based Systems | [4493441 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493441) | Important | Remote Code Execution | 4489886 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4493458 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493458) [4493471 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4493471) | Important | Remote Code Execution | 4489880 | Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

**声 明**

=============

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

**关于绿盟科技**

==============

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于2000年4月，总部位于北京。在国内外设有30多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及Web安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于2014年1月29日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

 

绿盟科技官方微博二维码 绿盟科技官方微信二维码