**微软发布6月补丁修复52个安全问题**

**安全威胁通告**



发布时间：2018年6月13日

## 综述

微软于周二发布了6月安全更新补丁，修复了52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Adobe Flash Player、Device Guard、HID Parser Library、Internet Explorer、Microsoft Edge、Microsoft NTFS、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows、Windows Hyper-V、Windows Kernel以及Windows Shell。

相关信息如下（红色部分威胁相对比较高）：

|  |  |  |
| --- | --- | --- |
| 产品 | CVE 编号 | CVE 标题 |
| Adobe Flash Player | ADV180014 | June 2018 Adobe Flash 安全更新 |
| Device Guard | CVE-2018-8201 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| Device Guard | CVE-2018-8211 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| Device Guard | CVE-2018-8212 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| Device Guard | CVE-2018-8215 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| Device Guard | CVE-2018-8216 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| Device Guard | CVE-2018-8217 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| Device Guard | CVE-2018-8221 | Device Guard Code Integrity Policy 安全功能绕过漏洞 |
| HID Parser Library | CVE-2018-8169 | HIDParser 特权提升漏洞 |
| Internet Explorer | CVE-2018-0978 | Internet Explorer 内存破坏漏洞 |
| Internet Explorer | CVE-2018-8113 | Internet Explorer 安全功能绕过漏洞 |
| Internet Explorer | CVE-2018-8249 | Internet Explorer 内存破坏漏洞 |
| Microsoft Edge | CVE-2018-0871 | Microsoft Edge 信息泄露漏洞 |
| Microsoft Edge | CVE-2018-8110 | Microsoft Edge 内存破坏漏洞 |
| Microsoft Edge | CVE-2018-8111 | Microsoft Edge 内存破坏漏洞 |
| Microsoft Edge | CVE-2018-8234 | Microsoft Edge 信息泄露漏洞 |
| Microsoft Edge | CVE-2018-8235 | Microsoft Edge 安全功能绕过漏洞 |
| Microsoft Edge | CVE-2018-8236 | Microsoft Edge 内存破坏漏洞 |
| Microsoft NTFS | CVE-2018-1036 | NTFS 特权提升漏洞 |
| Microsoft Office | CVE-2018-8244 | Microsoft Outlook 特权提升漏洞 |
| Microsoft Office | CVE-2018-8245 | Microsoft Office 特权提升漏洞 |
| Microsoft Office | CVE-2018-8246 | Microsoft Excel 信息泄露漏洞 |
| Microsoft Office | CVE-2018-8247 | Microsoft Office 特权提升漏洞 |
| Microsoft Office | CVE-2018-8248 | Microsoft Excel 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-8252 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-8254 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | ADV180015 | Microsoft Office Defense in Depth Update |
| Microsoft Scripting Engine | CVE-2018-8227 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-8229 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-8243 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-8267 | Scripting Engine 内存破坏漏洞 |
| Microsoft Windows | CVE-2018-8175 | WEBDAV 拒绝服务漏洞 |
| Microsoft Windows | CVE-2018-8205 | Windows 拒绝服务漏洞 |
| Microsoft Windows | CVE-2018-8208 | Windows Desktop Bridge 特权提升漏洞 |
| Microsoft Windows | CVE-2018-8209 | Windows Wireless Network Profile 信息泄露漏洞 |
| Microsoft Windows | CVE-2018-8210 | Windows 远程代码执行漏洞 |
| Microsoft Windows | CVE-2018-8213 | Windows 远程代码执行漏洞 |
| Microsoft Windows | CVE-2018-8214 | Windows Desktop Bridge 特权提升漏洞 |
| Microsoft Windows | CVE-2018-8225 | Windows DNSAPI 远程代码执行漏洞 |
| Microsoft Windows | CVE-2018-8226 | HTTP.sys 拒绝服务漏洞 |
| Microsoft Windows | CVE-2018-8231 | HTTP Protocol Stack 远程代码执行漏洞 |
| Microsoft Windows | CVE-2018-8239 | Windows GDI 信息泄露漏洞 |
| Microsoft Windows | CVE-2018-0982 | Windows 特权提升漏洞 |
| Microsoft Windows | CVE-2018-1040 | Windows Code Integrity Module 拒绝服务漏洞 |
| Microsoft Windows | CVE-2018-8251 | Media Foundation 内存破坏漏洞 |
| Windows Hyper-V | CVE-2018-8218 | Windows Hyper-V 拒绝服务漏洞 |
| Windows Hyper-V | CVE-2018-8219 | Hypervisor Code Integrity 特权提升漏洞 |
| Windows Kernel | CVE-2018-8207 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-8224 | Windows Kernel 特权提升漏洞 |
| Windows Kernel | CVE-2018-8233 | Win32k 特权提升漏洞 |
| Windows Kernel | CVE-2018-8121 | Windows Kernel 信息泄露漏洞 |
| Windows Shell | CVE-2018-8140 | Cortana 特权提升漏洞 |

## 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

# ADV180014 - June 2018 Adobe Flash Security Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV180014 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV180014) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV180014) | **CVE Title:** June 2018 Adobe Flash Security Update  **Description:**  This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin [APSB18-19](http://helpx.adobe.com/security/products/flash-player/apsb18-19.html): CVE-2018-4945, CVE-2018-5000, CVE-2018-5001, CVE-2018-5002.  **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    06/07/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **ADV180014** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Adobe Flash Player on Windows Server 2012 | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for 32-bit systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for x64-based systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2012 R2 | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows RT 8.1 | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for 32-bit Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for x64-based Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2016 | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1803 for 32-bit Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1803 for x64-based Systems | [4287903 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4287903) | Critical | Remote Code Execution | 4103729 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# ADV180015 - Microsoft Office Defense in Depth Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV180015 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV180015) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV180015) | **CVE Title:** Microsoft Office Defense in Depth Update  **Description:**  Microsoft has released an update for Microsoft Office that provides enhanced security as a defense in depth measure. This update improves the memory handling of Office applications that render Office Art.  **FAQ:**  **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?**  When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.  For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table.  For more information on this behavior and recommended actions, see [Microsoft Knowledge Base Article 830335](https://support.microsoft.com/kb/830335). For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | None | Defense in Depth |

## Affected Software

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

| **ADV180015** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [3115197 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c9a48d72-f3fe-4225-a484-e6a39f273031) [3115248 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=76f056ae-059c-4ec8-a8c8-ec13794369d5) | None | Defense in Depth | 3054984 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [3115197 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d27748a3-edd1-40dc-acbe-82ca10d9d46c) [3115248 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1d44791a-da9b-47da-8352-2c56c87f8046) | None | Defense in Depth | 3054984 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4018387 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ab24f7ad-3fe4-4f0a-b20e-00f591badf0e) | None | Defense in Depth | 4018288 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4018387 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4496fe7a-b295-4141-acf8-9a8b1fec8617) | None | Defense in Depth | 4018288 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4018387 Security Update | None | Defense in Depth | 4018288 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps Server 2013 Service Pack 1 | [4022183 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=dfa7070c-e809-4397-9574-15d54970acd9) | None | Defense in Depth | 4018393 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps Server 2010 Service Pack 2 | [4022203 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b3716982-5bab-4595-bb42-b2752ded38fe) | None | Defense in Depth | 4022142 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Excel Services on Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4018391 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9309f970-bf79-4e4f-88e3-8d0d4343ab46) | None | Defense in Depth | 4018343 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 2 | [4022197 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6e8d3482-be9a-4e52-b050-f690a19474f5) | None | Defense in Depth | 4022135 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Word Automation Services on Microsoft SharePoint Server 2013 Service Pack 1 | [4022179 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1307d832-3d79-4bfd-b8ed-c97fee01216c) | None | Defense in Depth | 4018388 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0871 - Microsoft Edge Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0871 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0871) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0871) | **CVE Title:** Microsoft Edge Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Edge improperly marks files.  An attacker who successfully exploited this vulnerability could exfiltrate file contents from disk. For an attack to be successful, an attacker must persuade a user to open a malicious website.  The security update addresses the vulnerability by properly marking files.  **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 unauthorized file system access - reading from file system.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0871** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 | Yes |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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 | Yes |
| Microsoft Edge on Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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 | Yes |

# CVE-2018-0978 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0978 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0978) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0978) | **CVE Title:** Internet Explorer Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.  An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.  The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0978** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Low | Remote Code Execution | 4103768 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Low | Remote Code Execution | 4103768 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Remote Code Execution | 4103718 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Remote Code Execution | 4103718 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Low | Remote Code Execution | 4103718 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Important | Remote Code Execution | 4103768 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) | Important | Remote Code Execution | 4103725 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) | Low | Remote Code Execution | 4103725 | 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 | 4284815 Monthly Rollup | Important | Remote Code Execution | 4103725 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Remote Code Execution | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Remote Code Execution | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Low | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Remote Code Execution | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Remote Code Execution | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Remote Code Execution | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | 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 | [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Low | Remote Code Execution | 4103768 | 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 |

# CVE-2018-0982 - Windows Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0982 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0982) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0982) | **CVE Title:** Windows Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the way that the Windows Kernel API enforces permissions. An attacker who successfully exploited the vulnerability could impersonate processes, interject cross-process communication, or interrupt system functionality.  To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.  The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly enforces permissions.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-0982** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | 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-2018-1036 - NTFS Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1036 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1036) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1036) | **CVE Title:** NTFS Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when NTFS improperly checks access. An attacker who successfully exploited this vulnerability could run processes in an elevated context.  To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system.  The security update addresses the vulnerability by correcting how NTFS checks access.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1036** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103718 | 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 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Elevation of Privilege | 4103730 | 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) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Elevation of Privilege | 4103730 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | 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 | 4284815 Monthly Rollup | Important | Elevation of Privilege | 4103725 | 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) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Elevation of Privilege | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Elevation of Privilege | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | 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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103721 | 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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103721 | 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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103721 | 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) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103721 | 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-2018-1040 - Windows Code Integrity Module Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1040 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1040) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1040) | **CVE Title:** Windows Code Integrity Module Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists in the way that the Windows Code Integrity Module performs hashing.  An attacker who successfully exploited the vulnerability could cause a system to stop responding. Note that the denial of service condition would not allow an attacker to execute code or to elevate user privileges. However, the denial of service condition could prevent authorized users from using system resources.  An attacker could host a specially crafted file in a website or SMB share. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases 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 via an enticement in email or instant message, or by getting them to open an email attachment.  The security update addresses the vulnerability by modifying how the Code Integrity Module performs hashing.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-1040** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Denial of Service | 4103718 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2012 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Denial of Service | 4103730 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2012 (Server Core installation) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Denial of Service | 4103730 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 8.1 for 32-bit systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 8.1 for x64-based systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2012 R2 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows RT 8.1 | 4284815 Monthly Rollup | Important | Denial of Service | 4103725 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Denial of Service | 4103716 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Denial of Service | 4103716 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Denial of Service | 4103731 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Denial of Service | 4103731 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O | Yes |

# CVE-2018-8110 - Microsoft Edge Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8110 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8110) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8110) | **CVE Title:** Microsoft Edge Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to 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 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.  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 by adding specially crafted content that could exploit the vulnerability. 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 way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email.  The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8110** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 |

# CVE-2018-8111 - Microsoft Edge Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8111 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8111) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8111) | **CVE Title:** Microsoft Edge Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to 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 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.  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 by adding specially crafted content that could exploit the vulnerability. 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 way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email.  The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8111** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 |

# CVE-2018-8113 - Internet Explorer Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8113 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8113) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8113) | **CVE Title:** Internet Explorer Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Internet Explorer that allows for bypassing Mark of the Web Tagging (MOTW). Failing to set the MOTW means that a large number of Microsoft security technologies are bypassed.  In a web-based attack scenario, an attacker could host a malicious website that is designed to exploit the security feature bypass. Alternatively, in an email or instant message attack scenario, the attacker could send the targeted user a specially crafted .url file that is designed to exploit the bypass. Additionally, compromised websites or websites that accept or host user-provided content could contain specially crafted content to exploit the security feature bypass. However, in all cases an attacker would have no way to force a user to view attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could entice a user to either click a link that directs the user to the attacker's site or send a malicious attachment.  The security update addresses the security feature bypass by correcting how Internet Explorer handles MOTW tagging.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8113** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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-2018-8121 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8121 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8121) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8121) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.  To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  The update addresses the vulnerability by correcting how the Windows kernel initializes 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    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-8121** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | Base: 4.7 Temporal: 4.5 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/RL:O | Yes |

# CVE-2018-8140 - Cortana Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8140 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8140) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8140) | **CVE Title:** Cortana Elevation of Privilege Vulnerability  **Description:**  An Elevation of Privilege vulnerability exists when Cortana retrieves data from user input services without consideration for status. An attacker who successfully exploited the vulnerability could execute commands with elevated permissions.  To exploit the vulnerability, an attacker would require physical/console access and the system would need to have Cortana assistance enabled.  The security update addresses the vulnerability by ensuring Cortana considers status when retrieves information from input services.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8140** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 6.8 Temporal: 5.9 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 6.8 Temporal: 5.9 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 6.8 Temporal: 5.9 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 6.8 Temporal: 5.9 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 6.8 Temporal: 5.9 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 6.8 Temporal: 5.9 Vector: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Yes |

# CVE-2018-8169 - HIDParser Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8169 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8169) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8169) | **CVE Title:** HIDParser Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when the (Human Interface Device) HID Parser Library driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.  To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system.  The security update addresses the vulnerability by correcting how the HID Parser Library handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8169** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4294413 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4294413) | Important | Elevation of Privilege | 4103718 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2012 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Elevation of Privilege | 4103730 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2012 (Server Core installation) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Elevation of Privilege | 4103730 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 8.1 for 32-bit systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 8.1 for x64-based systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2012 R2 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows RT 8.1 | 4284815 Monthly Rollup | Important | Elevation of Privilege | 4103725 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Elevation of Privilege | 4103725 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Elevation of Privilege | 4103716 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Elevation of Privilege | 4103716 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4294413 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4294413) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4294413 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4294413) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4294413 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4294413) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4294413 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4294413) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:O | Yes |

# CVE-2018-8175 - WEBDAV Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8175 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8175) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8175) | **CVE Title:** WEBDAV Denial of Service Vulnerability  **Description:**  An denial of service vulnerability exists when Windows NT WEBDAV Minirdr attempts to query a WEBDAV directory. An attacker who successfully exploited the vulnerability could cause a denial of service.  To exploit the vulnerability, an attacker could host a specially crafted website and then convince a user to browse to it, which would cause the victim's system to stop responding. However, an attacker could not 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 WEBDAV directory.  The security update addresses the vulnerability by correcting how Windows NT WEBDAV Minirdr attempts to query a WEBDAV directory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8175** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | Base: 5.9 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | Base: 5.9 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | Base: 5.9 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | Base: 5.9 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | Base: 5.9 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | Base: 5.9 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Yes |

# CVE-2018-8201 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8201 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8201) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8201) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8201** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | Base: 4.5 Temporal: 3.9 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C | Yes |

# CVE-2018-8205 - Windows Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8205 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8205) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8205) | **CVE Title:** Windows Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding.  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 cause a target system to stop responding.  The update addresses the vulnerability by correcting how Windows handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-8205** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Denial of Service | 4103718 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Denial of Service | 4103730 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Denial of Service | 4103730 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4284815 Monthly Rollup | Important | Denial of Service | 4103725 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Denial of Service | 4103725 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Denial of Service | 4103716 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Denial of Service | 4103716 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Denial of Service | 4103731 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Denial of Service | 4103731 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-8207 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8207 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8207) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8207) | **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 Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-8207** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Information Disclosure | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Information Disclosure | 4103718 | 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) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Information Disclosure | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Information Disclosure | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Information Disclosure | 4103718 | 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) | [4234459 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4234459) | Important | Information Disclosure | 4103718 | 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 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Information Disclosure | 4103730 | 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) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Information Disclosure | 4103730 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Information Disclosure | 4103725 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Information Disclosure | 4103725 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Information Disclosure | 4103725 | 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 | 4284815 Monthly Rollup | Important | Information Disclosure | 4103725 | 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) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Information Disclosure | 4103725 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Information Disclosure | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Information Disclosure | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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 | [4234459 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4234459) | Important | Information Disclosure | 4103721 | 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 | [4234459 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4234459) | Important | Information Disclosure | 4103721 | 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 | [4234459 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4234459) | Important | Information Disclosure | 4103721 | 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) | [4234459 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4234459) | Important | Information Disclosure | 4103721 | 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-2018-8208 - Windows Desktop Bridge Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8208 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8208) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8208) | **CVE Title:** Windows Desktop Bridge Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry. 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 the Windows Desktop Bridge manages the virtual registry.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8208** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |

# CVE-2018-8209 - Windows Wireless Network Profile Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8209 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8209) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8209) | **CVE Title:** Windows Wireless Network Profile Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Windows allows a normal user to access the Wireless LAN profile of an administrative user.  An authenticated attacker who successfully exploited the vulnerability could access the Wireless LAN profile of an administrative user, including passwords for wireless networks. An attacker would need to log on to the affected system and run a specific command.  The security update addresses the vulnerability by changing the way that Windows enforces access permissions to Wireless LAN profiles.  **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 unauthorized file system access - reading from file system.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-8209** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Information Disclosure | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Information Disclosure | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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-2018-8210 - Windows Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8210 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8210) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8210) | **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 these vulnerabilities could take control of an affected system.  To exploit the vulnerabilities, an attacker would first have to log on to the target system and then run a specially crafted application.  The updates address the vulnerabilities by correcting how Windows handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8210** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2012 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Remote Code Execution | 4103730 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Important | Remote Code Execution | 4103730 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Remote Code Execution | 4103725 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Remote Code Execution | 4103725 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Remote Code Execution | 4103725 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4284815 Monthly Rollup | Important | Remote Code Execution | 4103725 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Important | Remote Code Execution | 4103725 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Remote Code Execution | 4103716 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Remote Code Execution | 4103716 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Remote Code Execution | 4103723 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Remote Code Execution | 4103723 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Remote Code Execution | 4103723 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Remote Code Execution | 4103723 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Remote Code Execution | 4103731 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Remote Code Execution | 4103731 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-8211 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8211 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8211) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8211) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8211** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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-2018-8212 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8212 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8212) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8212) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8212** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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-2018-8213 - Windows Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8213 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8213) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8213) | **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 these vulnerabilities could take control of an affected system.  To exploit the vulnerabilities, an attacker would first have to log on to the target system and then run a specially crafted application.  The updates address the vulnerabilities by correcting how Windows handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8213** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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-2018-8214 - Windows Desktop Bridge Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8214 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8214) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8214) | **CVE Title:** Windows Desktop Bridge Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry. 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 the Windows Desktop Bridge manages the virtual registry.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8214** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |

# CVE-2018-8215 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8215 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8215) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8215) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8215** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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-2018-8216 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8216 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8216) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8216) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8216** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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-2018-8217 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8217 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8217) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8217) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8217** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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-2018-8218 - Windows Hyper-V Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8218 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8218) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8218) | **CVE Title:** Windows Hyper-V Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash.  To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash.  The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-8218** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.7 Temporal: 5.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-8219 - Hypervisor Code Integrity Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8219 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8219) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8219) | **CVE Title:** Hypervisor Code Integrity Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows Hyper-V instruction emulation fails to properly enforce privilege levels. An attacker who successfully exploited this vulnerability could gain elevated privileges on a target guest operating system. The host operating system is not vulnerable to this attack.  This vulnerability by itself does not allow arbitrary code to be run. However, the vulnerability could be used in conjunction with one or more vulnerabilities (e.g. a remote code execution vulnerability and another elevation of privilege) that could take advantage of the elevated privileges when running.  The update addresses the vulnerability by correcting how privileges are enforced by Windows Hyper-V instruction emulation.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8219** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Elevation of Privilege | 4103723 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Elevation of Privilege | 4103731 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Elevation of Privilege | 4103727 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7.6 Temporal: 6.8 Vector: CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-8221 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8221 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8221) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8221) | **CVE Title:** Device Guard Code Integrity Policy Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Device Guard that could allow an attacker to inject malicious code into a Windows PowerShell session. An attacker who successfully exploited this vulnerability could inject code into a trusted PowerShell process to bypass the Device Guard Code Integrity policy on the local machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then inject malicious code into a script that is trusted by the Code Integrity policy. The injected code would then run with the same trust level as the script and bypass the Code Integrity policy.  The update addresses the vulnerability by correcting how PowerShell exposes functions and processes user supplied code.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8221** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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-2018-8224 - Windows Kernel Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8224 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8224) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8224) | **CVE Title:** Windows Kernel Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when the Windows kernel 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 to take control of an affected system.  The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8224** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Important | Elevation of Privilege | 4103718 | 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) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103718 | 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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103718 | 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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103718 | 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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103718 | 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) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Important | Elevation of Privilege | 4103718 | 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-2018-8225 - Windows DNSAPI Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8225 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8225) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8225) | **CVE Title:** Windows DNSAPI Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in Windows [Domain Name System (DNS)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#DNS) DNSAPI.dll when it fails to properly handle DNS responses. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account.  To exploit the vulnerability, the attacker would use a malicious DNS server to send corrupted DNS responses to the target.  The update addresses the vulnerability by modifying how Windows DNSAPI.dll handles DNS responses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8225** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Critical | Remote Code Execution | 4103718 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Critical | Remote Code Execution | 4103730 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Critical | Remote Code Execution | 4103730 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4284815 Monthly Rollup | Critical | Remote Code Execution | 4103725 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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 | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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) | [4230467 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230467) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-8226 - HTTP.sys Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8226 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8226) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8226) | **CVE Title:** HTTP.sys Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists in the HTTP 2.0 protocol stack (HTTP.sys) when HTTP.sys improperly parses specially crafted HTTP 2.0 requests. An attacker who successfully exploited the vulnerability could create a denial of service condition, causing the target system to become unresponsive.  To exploit this vulnerability, an attacker could send a specially crafted HTTP packet to a target system, causing the affected system to become nonresponsive.  The update addresses the vulnerability by modifying how the Windows HTTP protocol stack handles HTTP 2.0 requests. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate user rights.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-8226** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Denial of Service | 4103716 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Denial of Service | 4103716 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Denial of Service | 4103723 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Denial of Service | 4103731 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Denial of Service | 4103731 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Denial of Service | 4103727 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Denial of Service | 4103721 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2018-8227 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8227 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8227) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8227) | **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    06/12/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8227** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Remote Code Execution | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Remote Code Execution | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Remote Code Execution | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Remote Code Execution | 4103721 | 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 | [Commit Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.5) | Important | Remote Code Execution | 4103721 | 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 |

# CVE-2018-8229 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8229 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8229) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8229) | **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    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8229** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Moderate | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [Commit Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.5) | Critical | Remote Code Execution | 4103721 | 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 |

# CVE-2018-8231 - HTTP Protocol Stack Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8231 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8231) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8231) | **CVE Title:** HTTP Protocol Stack Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when HTTP Protocol Stack (Http.sys) improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code and take control of the affected system.  To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted Http.sys server.  The security update fixes this vulnerability by correcting how HTTP Protocol Stack(Http.sys) handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8231** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | Base: 8.1 Temporal: 7.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/RL:O/RC:C | Yes |

# CVE-2018-8233 - Win32k Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8233 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8233) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8233) | **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    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8233** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Elevation of Privilege | 4103721 | Base: 7.8 Temporal: 7.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | Yes |

# CVE-2018-8234 - Microsoft Edge Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8234 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8234) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8234) | **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    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-8234** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Information Disclosure | 4103716 | 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 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Information Disclosure | 4103716 | 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 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Low | Information Disclosure | 4103723 | 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 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | 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 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | 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 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | 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 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | 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-2018-8235 - Microsoft Edge Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8235 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8235) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8235) | **CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists when Microsoft Edge improperly handles requests of different origins. The vulnerability allows Microsoft Edge to bypass Same-Origin Policy (SOP) restrictions, and to allow requests that should otherwise be ignored. An attacker who successfully exploited the vulnerability could force the browser to send data that would otherwise be restricted.  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 affected Microsoft Edge handles different-origin requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8235** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Important | Security Feature Bypass | 4103716 | 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 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Low | Security Feature Bypass | 4103723 | 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 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Security Feature Bypass | 4103723 | 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 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Security Feature Bypass | 4103731 | 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 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Security Feature Bypass | 4103727 | 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 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Security Feature Bypass | 4103721 | 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-2018-8236 - Microsoft Edge Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8236 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8236) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8236) | **CVE Title:** Microsoft Edge Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to 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 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.  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 by adding specially crafted content that could exploit the vulnerability. 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 way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email.  The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8236** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Moderate | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 |

# CVE-2018-8239 - Windows GDI Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8239 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8239) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8239) | **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 memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-8239** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Important | Information Disclosure | 4103723 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Important | Information Disclosure | 4103731 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Important | Information Disclosure | 4103727 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Important | Information Disclosure | 4103721 | Base: 4.4 Temporal: 4.4 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N | Yes |

# CVE-2018-8243 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8243 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8243) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8243) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the ChakraCore scripting 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.  The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8243** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ChakraCore | [Commit Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.5) | Critical | Remote Code Execution |  | Base: 8.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | Yes |

# CVE-2018-8244 - Microsoft Outlook Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8244 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8244) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8244) | **CVE Title:** Microsoft Outlook Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft Outlook does not validate attachment headers properly. An attacker who successfully exploited the vulnerability could send an email with hidden attachments that would be opened or executed once a victim clicks a link within the email. Note that this does not bypass attachment filters, so blocked attachments will still be excluded.  To exploit the vulnerability, the attacker could send a specially crafted email to a victim. The victim would then be required to click on a link within the email to open or execute a malicious attachment.  This update addresses the vulnerability by changing the way that Outlook parses attachment headers.  **FAQ:**  **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?**  When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.  For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table.  For more information on this behavior and recommended actions, see [Microsoft Knowledge Base Article 830335](https://support.microsoft.com/kb/830335). For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8244** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Outlook 2013 RT Service Pack 1 | 4022169 Security Update | Important | Elevation of Privilege | 4011697 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Outlook 2010 Service Pack 2 (32-bit editions) | [4022205 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=32e49f35-bfca-4c57-80c1-a7fe200a0ae4) | Important | Elevation of Privilege | 4011711 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Outlook 2010 Service Pack 2 (64-bit editions) | [4022205 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4164aec8-c385-4025-9790-368f3fdbf11c) | Important | Elevation of Privilege | 4011711 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Outlook 2016 (32-bit edition) | [4022160 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=78c6e5fd-6021-488d-8b83-a94de9d82d4d) | Important | Elevation of Privilege | 4011682 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Outlook 2016 (64-bit edition) | [4022160 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b94f491e-613c-44d6-975c-ff980f43473f) | Important | Elevation of Privilege | 4011682 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Outlook 2013 Service Pack 1 (32-bit editions) | [4022169 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d6c89db4-f152-432f-abf3-48c16eaf2c63) | Important | Elevation of Privilege | 4011697 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Outlook 2013 Service Pack 1 (64-bit editions) | [4022169 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=a9924498-c55b-4ac8-b35c-7bf142449556) | Important | Elevation of Privilege | 4011697 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Elevation of Privilege | 4011697 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Elevation of Privilege | 4011697 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-8245 - Microsoft Office Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8245 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8245) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8245) | **CVE Title:** Microsoft Office Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft Publisher fails to utilize features that lock down the Local Machine zone when instantiating OLE objects. An attacker who successfully exploited the vulnerability could force arbitrary code to be executed in the Local Machine zone.  To exploit the vulnerability, the attacker could send a specially crafted Publisher document to a victim. The user would then need to open the document in Publisher to trigger the vulnerability.  This update addresses the vulnerability by ensuring that Publisher properly utilizes built-in OS functionality to lock down the Local Machine zone.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8245** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Publisher 2010 Service Pack 2 (32-bit editions) | [4011186 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b9b57872-f106-4226-8f3b-8fca86843363) | Important | Elevation of Privilege | 3141537 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Publisher 2010 Service Pack 2 (64-bit editions) | [4011186 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c2b0fadc-a7db-4243-9201-aeb87cb5e881) | Important | Elevation of Privilege | 3141537 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-8246 - Microsoft Excel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8246 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8246) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8246) | **CVE Title:** Microsoft Excel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the userâ€™s computer or data.  To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created.  The update addresses the vulnerability by changing the way certain Excel functions 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 uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process.  **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?**  When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.  For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table.  For more information on this behavior and recommended actions, see [Microsoft Knowledge Base Article 830335](https://support.microsoft.com/kb/830335). For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-8246** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4022209 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f1ab5397-f864-44e4-b3ae-e10874271c2e) | Important | Information Disclosure | 4022146 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4022209 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b0007073-bbf1-4157-86e0-4d5ac0afbb97) | Important | Information Disclosure | 4022146 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4022199 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=8b2e0625-909b-4182-8407-5776e2c2cf3f) | Important | Information Disclosure | 2899590 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4022199 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4ccee781-48a0-427f-8905-91a18230d8a8) | Important | Information Disclosure | 2899590 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | [4022191 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d34b7660-58ea-4f60-81b7-caa37f80daec) | Important | Information Disclosure | 4018399 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | [4022191 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=8b6c6d92-77f0-4f09-a82c-a505f645a7be) | Important | Information Disclosure | 4018399 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4022191 Security Update | Important | Information Disclosure | 4018399 | Base: N/A Temporal: N/A Vector: N/A | Unknown |
| Microsoft Excel 2016 (32-bit edition) | [4022174 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=20ca33ec-8065-4ef9-846d-6592499f5d36) | Important | Information Disclosure | 4018382 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | [4022174 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c95e9200-0b2f-47fe-a63a-170deecfe8fc) | Important | Information Disclosure | 4018382 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel Viewer | [4022151 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=feb298a4-232d-417b-b5e3-6196aa5d24a5) | Important | Information Disclosure | 4011719 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | 4011719 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | 4011719 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office Compatibility Pack Service Pack 3 | [4022196 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ec47f04f-4000-4e29-9ad8-b140976b6da7) | Important | Information Disclosure | 4022150 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-8247 - Microsoft Office Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8247 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8247) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8247) | **CVE Title:** Microsoft Office Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Office Web Apps Server 2013 and Office Online Server fail to properly handle web requests. An attacker who successfully exploited this vulnerability could perform script/content injection attacks and attempt to trick the user into disclosing sensitive information.  To exploit the vulnerability, an attacker could send an email message containing a malicious link to a user. Alternatively, an attacker could use a chat client to social engineer a user into clicking the malicious link. The user must click the malicious link for the vulnerability to be exploited.  The security update addresses the vulnerability by correcting how Office Web Apps Server 2013 and Office Online Server validate web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8247** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office Web Apps Server 2013 Service Pack 1 | [4022183 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=dfa7070c-e809-4397-9574-15d54970acd9) | Important | Elevation of Privilege | 4018393 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Online Server 2016 | [4011026 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=82183a7a-e8ed-4343-aea3-e392522ef5b5) | Important | Elevation of Privilege | 4011023 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-8248 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8248 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8248) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8248) | **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:**  **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?**  When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.  For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table.  For more information on this behavior and recommended actions, see [Microsoft Knowledge Base Article 830335](https://support.microsoft.com/kb/830335). For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8248** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4022199 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=8b2e0625-909b-4182-8407-5776e2c2cf3f) | Important | Remote Code Execution | 2899590 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4022199 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4ccee781-48a0-427f-8905-91a18230d8a8) | Important | Remote Code Execution | 2899590 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4022182 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9153279e-8c5f-48eb-b900-ef25db158bb6) | Important | Remote Code Execution | 3172436 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4022182 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=1792d767-99e2-4cc6-9b1d-68fc03ee2677) | Important | Remote Code Execution | 3172436 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4022182 Security Update | Important | Remote Code Execution | 3172436 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4022177 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=92e20498-9107-425b-b3b0-0fc8b3c74468) | Important | Remote Code Execution | 4018327 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4022177 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ad71db48-da94-4287-8a67-29820dc3ba50) | Important | Remote Code Execution | 4018327 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018327 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4018327 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-8249 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8249 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8249) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8249) | **CVE Title:** Internet Explorer Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.  An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.  The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8249** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Moderate | Remote Code Execution | 4103718 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Critical | Remote Code Execution | 4103768 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) | Critical | Remote Code Execution | 4103725 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) | Moderate | Remote Code Execution | 4103725 | 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 | 4284815 Monthly Rollup | Critical | Remote Code Execution | 4103725 | 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-2018-8251 - Media Foundation Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8251 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8251) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8251) | **CVE Title:** Media Foundation Memory Corruption Vulnerability  **Description:**  A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory. An attacker who successfully exploited the vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights.  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 a malicious webpage.  The security update addresses the vulnerability by correcting how Windows Media Foundation handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8251** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 |
| Windows 7 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4284867 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284867) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 |
| Windows Server 2012 | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Critical | Remote Code Execution | 4103730 | 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 |
| Windows Server 2012 (Server Core installation) | [4284846 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284846) [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) | Critical | Remote Code Execution | 4103730 | 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 |
| Windows 8.1 for 32-bit systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | 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 |
| Windows 8.1 for x64-based systems | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | 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 |
| Windows Server 2012 R2 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | 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 |
| Windows RT 8.1 | 4284815 Monthly Rollup | Critical | Remote Code Execution | 4103725 | 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 |
| Windows Server 2012 R2 (Server Core installation) | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4284878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284878) | Critical | Remote Code Execution | 4103725 | 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 |
| Windows 10 for 32-bit Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 |
| Windows 10 for x64-based Systems | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 |
| Windows Server 2016 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 |
| Windows 10 Version 1607 for 32-bit Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 |
| Windows 10 Version 1607 for x64-based Systems | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 |
| Windows Server 2016 (Server Core installation) | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 |
| Windows 10 Version 1703 for 32-bit Systems | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 |
| Windows 10 Version 1709 for 32-bit Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 |
| Windows 10 Version 1709 for x64-based Systems | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 |
| Windows Server, version 1709 (Server Core Installation) | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 |
| Windows 10 Version 1803 for 32-bit Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 |
| Windows 10 Version 1803 for x64-based Systems | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 |
| Windows Server, version 1803 (Server Core Installation) | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 |

# CVE-2018-8252 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8252 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8252) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8252) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege 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. These 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:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8252** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Foundation 2013 Service Pack 1 | [4022190 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=12fcdc8c-8b6b-4e70-a0f0-08f38f566ff1) | Important | Elevation of Privilege | 4018398 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4022173 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6c98f154-340c-4d97-a625-842676decdbc) | Important | Elevation of Privilege | 4018381 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-8254 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8254 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8254) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8254) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege 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. These 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:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    06/12/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-8254** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2010 Service Pack 2 | [4022210 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=e1d7e9a1-7d81-4c81-b533-90b88130913e) | Important | Elevation of Privilege | 3114889 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Foundation 2013 Service Pack 1 | [4022190 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=12fcdc8c-8b6b-4e70-a0f0-08f38f566ff1) | Important | Elevation of Privilege | 4018398 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4022173 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6c98f154-340c-4d97-a625-842676decdbc) | Important | Elevation of Privilege | 4018381 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-8267 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8267 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8267) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8267) | **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    06/12/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-8267** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Moderate | Remote Code Execution | 4103768 | 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 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Moderate | Remote Code Execution | 4103768 | 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 7 for 32-bit Systems Service Pack 1 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Critical | Remote Code Execution | 4103718 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284826 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284826) | Moderate | Remote Code Execution | 4103718 | 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 | [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Critical | Remote Code Execution | 4103768 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) | Critical | Remote Code Execution | 4103725 | 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 | [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) [4284815 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284815) | Moderate | Remote Code Execution | 4103725 | 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 | 4284815 Monthly Rollup | Critical | Remote Code Execution | 4103725 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284860 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284860) | Critical | Remote Code Execution | 4103716 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Moderate | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284880 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284880) | Critical | Remote Code Execution | 4103723 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284874 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284874) | Critical | Remote Code Execution | 4103731 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284819 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284819) | Critical | Remote Code Execution | 4103727 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [4284835 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284835) | Critical | Remote Code Execution | 4103721 | 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 | [4284855 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4284855) [4230450 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4230450) | Moderate | Remote Code Execution | 4103768 | 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 |

**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