**微软发布4月补丁修复67个安全问题**

**安全威胁通告**



发布时间：2017年9月13日

## 综述

微软于周二发布了4月安全更新补丁，修复了67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、Internet Explorer、Microsoft Browsers、Microsoft Devices、Microsoft Edge、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Malware Protection Engine、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows、Visual Studio、Windows Hyper-V、Windows IIS、Windows Kernel以及Windows RDP。

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 | ADV180007 | April 2018 Adobe Flash 安全更新 |
| Internet Explorer | CVE-2018-0991 | Internet Explorer 内存破坏漏洞 |
| Internet Explorer | CVE-2018-0997 | Internet Explorer 内存破坏漏洞 |
| Internet Explorer | CVE-2018-0870 | Internet Explorer 内存破坏漏洞 |
| Internet Explorer | CVE-2018-1018 | Internet Explorer 内存破坏漏洞 |
| Internet Explorer | CVE-2018-1020 | Internet Explorer 内存破坏漏洞 |
| Microsoft Browsers | CVE-2018-1023 | Microsoft Browser 内存破坏漏洞 |
| Microsoft Devices | CVE-2018-8117 | Microsoft Wireless Keyboard 850 安全功能绕过漏洞 |
| Microsoft Edge | CVE-2018-0892 | Microsoft Edge 信息泄露漏洞 |
| Microsoft Edge | CVE-2018-0998 | Microsoft Edge 信息泄露漏洞 |
| Microsoft Graphics Component | CVE-2018-1009 | Microsoft DirectX Graphics Kernel Subsystem 特权提升漏洞 |
| Microsoft Graphics Component | CVE-2018-1010 | Microsoft Graphics 远程代码执行漏洞 |
| Microsoft Graphics Component | CVE-2018-1012 | Microsoft Graphics 远程代码执行漏洞 |
| Microsoft Graphics Component | CVE-2018-1013 | Microsoft Graphics 远程代码执行漏洞 |
| Microsoft Graphics Component | CVE-2018-1015 | Microsoft Graphics 远程代码执行漏洞 |
| Microsoft Graphics Component | CVE-2018-1016 | Microsoft Graphics 远程代码执行漏洞 |
| Microsoft JET Database Engine | CVE-2018-1003 | Microsoft JET Database Engine 远程代码执行漏洞 |
| Microsoft Malware Protection Engine | CVE-2018-0986 | Microsoft Malware Protection Engine 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-0950 | Microsoft Office 信息泄露漏洞 |
| Microsoft Office | CVE-2018-1032 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0920 | Microsoft Excel 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1005 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-1007 | Microsoft Office 信息泄露漏洞 |
| Microsoft Office | CVE-2018-1011 | Microsoft Excel 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1014 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-1026 | Microsoft Office 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1027 | Microsoft Excel 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1028 | Microsoft Office Graphics 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1029 | Microsoft Excel 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1030 | Microsoft Office 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-1034 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Scripting Engine | CVE-2018-0987 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2018-0988 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0989 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2018-0990 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0993 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0994 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0995 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0996 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-1000 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2018-1001 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-1004 | Windows VBScript Engine 远程代码执行漏洞 |
| Microsoft Scripting Engine | CVE-2018-0979 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0980 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0981 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2018-1019 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Windows | CVE-2018-0887 | Windows Kernel 信息泄露漏洞 |
| Microsoft Windows | CVE-2018-0890 | Active Directory 安全功能绕过漏洞 |
| Microsoft Windows | CVE-2018-0963 | Windows Kernel 特权提升漏洞 |
| Microsoft Windows | CVE-2018-0966 | Device Guard 安全功能绕过漏洞 |
| Microsoft Windows | CVE-2018-0967 | Windows SNMP Service 拒绝服务漏洞 |
| Microsoft Windows | CVE-2018-8116 | Microsoft Graphics Component 拒绝服务漏洞 |
| Visual Studio | CVE-2018-1037 | Microsoft Visual Studio 信息泄露漏洞 |
| Windows Hyper-V | CVE-2018-0957 | Hyper-V 信息泄露漏洞 |
| Windows Hyper-V | CVE-2018-0964 | Hyper-V 信息泄露漏洞 |
| Windows IIS | CVE-2018-0956 | HTTP.sys 拒绝服务漏洞 |
| Windows Kernel | CVE-2018-0960 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0968 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0969 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0970 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0971 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0972 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0973 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0974 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0975 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-1008 | OpenType Font Driver 特权提升漏洞 |
| Windows RDP | CVE-2018-0976 | Windows Remote Desktop Protocol (RDP) 拒绝服务漏洞 |

## 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

# ADV180007 - April 2018 Adobe Flash Security Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV180007 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV180007) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV180007) | **CVE Title:** April 2018 Adobe Flash Security Update  **Description:**  This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin [APSB18-08](http://helpx.adobe.com/security/products/flash-player/apsb18-08.html): CVE-2018-4932, CVE-2018-4933, CVE-2018-4934, CVE-2018-4935, CVE-2018-4936, and CVE-2018-4937.  **FAQ:**  **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit any of these vulnerabilities. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.  In a web-based attack scenario where the user is using Internet Explorer in the Windows 8-style UI, an attacker would first need to compromise a website already listed in the Compatibility View (CV) list. An attacker could then host a website that contains specially crafted Flash content designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. For more information about Internet Explorer and the CV List, please see the MSDN Article, Developer Guidance for websites with content for Adobe Flash Player in Windows 8.  **Mitigations:**  **Workarounds:**  Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update.  **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry.  **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps:   1. Paste the following into a text file and save it with the .reg file extension. 2. Windows Registry Editor Version 5.00 3. [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 4. "Compatibility Flags"=dword:00000400 5. [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 6. "Compatibility Flags"=dword:00000400 7. Double-click the .reg file to apply it to an individual system.   You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection.  **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround. **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy** **Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites:  [Group Policy Overview](https://technet.microsoft.com/library/hh831791) [What is Group Policy Object Editor?](https://technet.microsoft.com/library/cc737816%28v=ws.10%29.aspx) [Core Group Policy tools and settings](https://technet.microsoft.com/library/cc784165%28v=ws.10%29.aspx)  To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010.   1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to Enabled. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. **Prevent Adobe Flash Player from running in Office 2010 on affected systems** **Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.   To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps:   1. Create a text file named Disable\_Flash.reg with the following contents:   [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]  "Compatibility Flags"=dword:00000400   1. Double-click the .reg file to apply it to an individual system. 2. **Note** You must restart Internet Explorer for your changes to take effect. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, [Group Policy collection](http://go.microsoft.com/fwlink/?LinkID=215719). **Prevent ActiveX controls from running in Office 2007 and Office 2010**   To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps:   1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then select Disable all controls without notifications. 3. Click OK to save your settings. **Impact of workaround**. Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround**.   To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps:   1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then deselect Disable all controls without notifications. 3. Click OK to save your settings. **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High.   To raise the browsing security level in Internet Explorer, perform the following steps:   1. On the Internet Explorer **Tools** menu, click\*\* Internet Option\*\*s. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround**. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone**   You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps:   1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround**. There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.   To do this, perform the following steps:   1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are \***.windowsupdate.microsoft.com** and \***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update.   **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **ADV180007** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Adobe Flash Player on Windows Server 2012 | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for 32-bit systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for x64-based systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2012 R2 | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows RT 8.1 | 4093110 Security Update | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for 32-bit Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for x64-based Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2016 | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems | [4093110 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093110) | Critical | Remote Code Execution | 4088785 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2018-0870 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0870 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0870) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0870) | **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    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0870** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |

# CVE-2018-0887 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0887 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0887) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0887) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address. 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 security update addresses the vulnerability by correcting how the Windows kernel initializes memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0887** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0890 - Active Directory Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0890 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0890) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0890) | **CVE Title:** Active Directory Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists when Active Directory incorrectly applies Network Isolation settings. To exploit this vulnerability, an attacker could run a specially crafted application.  An attacker who successfully exploited this vulnerability could bypass firewall policies applied to Modern Applications.  This update corrects the security featureâ€™s behavior by correcting how Active Directory manages Network Isolation policies applied to Modern Applications.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-0890** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Security Feature Bypass | 4088782 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Security Feature Bypass | 4088782 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Security Feature Bypass | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Security Feature Bypass | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Security Feature Bypass | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0892 - Microsoft Edge Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0892 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0892) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0892) | **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:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0892** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Low | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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-2018-0920 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0920 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0920) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0920) | **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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0920** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=70ec98c7-1510-4064-b4a3-6fb6a6ffe203) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0a81ef86-07cf-40dc-9eb4-fd9ac7a269eb) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0950 - Microsoft Office Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0950 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0950) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0950) | **CVE Title:** Microsoft Office Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Office renders Rich Text Format (RTF) email messages containing OLE objects when a message is opened or previewed. This vulnerability could potentially result in the disclosure of sensitive information to a malicious site.  To exploit the vulnerability, an attacker would have to send an RTF-formatted email to a user and convince the user to open or preview the email. A connection to a remote SMB server could then be automatically initiated, enabling the attacker to brute-force attack the corresponding NTLM challenge and response in order to disclose the corresponding hash password.  The security update addresses the vulnerability by correcting how Office processes OLE objects.  **FAQ:**  **I have Microsoft Word 2010 installed. Why am I not being offered the 4018357 update?** The 4018357 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update.  **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    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0950** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Word 2007 Service Pack 3 | [4018355 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=def0d181-207b-4448-bc2c-6037043cbaed) | Important | Information Disclosure | 4011721 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (32-bit editions) | [4018359 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=03f4f40a-2fda-4592-a2b4-d67796e30dcd) | Important | Information Disclosure | 4011674 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (64-bit editions) | [4018359 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=342a1e75-d442-4db0-bc11-a23cf2a761d0) | Important | Information Disclosure | 4011674 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4018357 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=08789693-0ff3-49c0-be08-169bbffa1d59) | Important | Information Disclosure | 4011673 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4018357 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=e32b4aa2-4f4f-46e6-b80d-a9bfb224e576) | Important | Information Disclosure | 4011673 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 Service Pack 1 (32-bit editions) | [4018347 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=697b6fd0-1cd7-4e88-b376-5de6a8c256c3) | Important | Information Disclosure | 4011695 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 Service Pack 1 (64-bit editions) | [4018347 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=974a638e-9a56-49e9-8bbe-0f9b41371e01) | Important | Information Disclosure | 4011695 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 RT Service Pack 1 | 4018347 Security Update | Important | Information Disclosure | 4011695 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2016 (32-bit edition) | [4018339 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=bb18a0d7-d0e4-4d55-946b-a54e998567e7) | Important | Information Disclosure | 4011730 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2016 (64-bit edition) | [4018339 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=10ae22bb-c5a5-44d4-bc6a-eda33b417fcf) | Important | Information Disclosure | 4011730 | 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 | 4011730 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | 4011730 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office Compatibility Pack Service Pack 3 | [4018354 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c6fd1491-d0f0-4667-be62-a37b3f7069c7) | Important | Information Disclosure | 4011720 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0956 - HTTP.sys Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0956 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0956) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0956) | **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    04/10/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-0956** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Denial of Service | 4088786 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Denial of Service | 4088786 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Denial of Service | 4088779 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Denial of Service | 4088779 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Denial of Service | 4088782 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Denial of Service | 4088782 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0957 - Hyper-V Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0957 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0957) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0957) | **CVE Title:** Hyper-V Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information.  An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system.  The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0957** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0960 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0960 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0960) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0960) | **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:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0960** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0963 - Windows Kernel Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0963 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0963) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0963) | **CVE Title:** Windows Kernel Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.  To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.  The security update addresses the vulnerability by ensuring the Windows Kernel properly handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-0963** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Elevation of Privilege | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Elevation of Privilege | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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-2018-0964 - Hyper-V Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0964 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0964) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0964) | **CVE Title:** Hyper-V Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information.  An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system.  The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0964** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0966 - Device Guard Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0966 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0966) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0966) | **CVE Title:** Device Guard Security Feature Bypass Vulnerability  **Description:**  A security feature bypass exists when Device Guard incorrectly validates an untrusted file. An attacker who successfully exploited this vulnerability could make an unsigned file appear to be signed. Because Device Guard relies on the signature to determine the file is non-malicious, Device Guard could then allow a malicious file to execute.  In an attack scenario, an attacker could make an untrusted file appear to be a trusted file.  The update addresses the vulnerability by correcting how Device Guard handles untrusted files.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-0966** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Security Feature Bypass | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Security Feature Bypass | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Security Feature Bypass | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Security Feature Bypass | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Security Feature Bypass | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Security Feature Bypass | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Security Feature Bypass | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Security Feature Bypass | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Security Feature Bypass | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Security Feature Bypass | 4088776 | 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-2018-0967 - Windows SNMP Service Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0967 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0967) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0967) | **CVE Title:** Windows SNMP Service Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists in the way that Windows SNMP Service handles malformed SNMP traps.  An attacker who successfully exploited the vulnerability could cause a target 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.  The security update addresses the vulnerability by correcting how Windows SNMP Service processes SNMP traps.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-0967** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4091756 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4091756) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Denial of Service | 4088877 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Denial of Service | 4088877 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Denial of Service | 4088786 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Denial of Service | 4088786 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Denial of Service | 4088779 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Denial of Service | 4088779 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Denial of Service | 4088782 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Denial of Service | 4088782 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4091756 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4091756) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4091756 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4091756) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4091756 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4091756) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4091756 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4091756) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0968 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0968 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0968) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0968) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0968** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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-2018-0969 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0969 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0969) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0969) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0969** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0970 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0970 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0970) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0970) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0970** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0971 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0971 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0971) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0971) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0971** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0972 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0972 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0972) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0972) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0972** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0973 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0973 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0973) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0973) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0973** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0974 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0974 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0974) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0974) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0974** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0975 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0975 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0975) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0975) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0975** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Information Disclosure | 4088875 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Information Disclosure | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4088776 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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 | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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) | [4093478 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093478) | Important | Information Disclosure | 4073080 | 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-2018-0976 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0976 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0976) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0976) | **CVE Title:** Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RDP service on the target system to stop responding.  To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services.  The update addresses the vulnerability by correcting how RDP handles connection requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

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

| **CVE-2018-0976** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4093227 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093227) | Important | Denial of Service | 4088875 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Denial of Service | 4088877 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Denial of Service | 4088877 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Denial of Service | 4088876 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Denial of Service | 4088786 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Denial of Service | 4088786 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Denial of Service | 4088779 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Denial of Service | 4088779 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Denial of Service | 4088787 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Denial of Service | 4088782 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Denial of Service | 4088782 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4093227 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093227) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4093227 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093227) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4093227 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093227) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4093227 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093227) | Important | Denial of Service | 4088776 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0979 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0979 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0979) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0979) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0979** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-0980 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0980 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0980) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0980) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0980** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-0981 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0981 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0981) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0981) | **CVE Title:** Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure 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 provide an attacker with information to further compromise the user's computer or data.  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. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Moderate | Information Disclosure |

## Affected Software

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

| **CVE-2018-0981** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Information Disclosure | 4088876 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Information Disclosure | 4088786 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Information Disclosure | 4088786 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Information Disclosure | 4088779 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Information Disclosure | 4088779 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Information Disclosure | 4088787 | 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 | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Information Disclosure | 4088787 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Information Disclosure | 4088787 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Information Disclosure | 4088782 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Information Disclosure | 4088782 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Information Disclosure | 4088776 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Information Disclosure | 4088776 | Base: 6.4 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | Yes |

# CVE-2018-0986 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0986 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0986) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0986) | **CVE Title:** Microsoft Malware Protection Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption. An attacker who successfully exploited this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, a specially crafted file must be scanned by an affected version of the Microsoft Malware Protection Engine. There are many ways that an attacker could place a specially crafted file in a location that is scanned by the Microsoft Malware Protection Engine. For example, an attacker could use a website to deliver a specially crafted file to the victim's system that is scanned when the website is viewed by the user. An attacker could also deliver a specially crafted file via an email message or in an Instant Messenger message that is scanned when the file is opened. In addition, an attacker could take advantage of websites that accept or host user-provided content, to upload a specially crafted file to a shared location that is scanned by the Malware Protection Engine running on the hosting server.  If the affected antimalware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, leading to exploitation of the vulnerability when the specially crafted file is scanned. If real-time scanning is not enabled, the attacker would need to wait until a scheduled scan occurs in order for the vulnerability to be exploited. All systems running an affected version of antimalware software are primarily at risk.  The update addresses the vulnerability by correcting the manner in which the Microsoft Malware Protection Engine scans specially crafted files.  Note: Typically, no action is required of enterprise administrators or end users to install updates for the Microsoft Malware Protection Engine, because the built-in mechanism for the automatic detection and deployment of updates will apply the update within 48 hours of release. The exact time frame depends on the software used, Internet connection, and infrastructure configuration.  **FAQ:**   | **References** | **Identification** | | --- | --- | | Last version of the Microsoft Malware Protection Engine affected by this vulnerability | Version 1.1.14600.4 | | First version of the Microsoft Malware Protection Engine with this vulnerability addressed | Version 1.1.14700.5 |   **Why is no action required to install this update?** In response to a constantly changing threat landscape, Microsoft frequently updates malware definitions and the Microsoft Malware Protection Engine. In order to be effective in helping protect against new and prevalent threats, antimalware software must be kept up to date with these updates in a timely manner.  For enterprise deployments as well as end users, the default configuration in Microsoft antimalware software helps ensure that malware definitions and the Microsoft Malware Protection Engine are kept up to date automatically. Product documentation also recommends that products are configured for automatic updating.  Best practices recommend that customers regularly verify whether software distribution, such as the automatic deployment of Microsoft Malware Protection Engine updates and malware definitions, is working as expected in their environment.  **How often are the Microsoft Malware Protection Engine and malware definitions updated?** Microsoft typically releases an update for the Microsoft Malware Protection Engine once a month or as needed to protect against new threats. Microsoft also typically updates the malware definitions three times daily and can increase the frequency when needed.  Depending on which Microsoft antimalware software is used and how it is configured, the software may search for engine and definition updates every day when connected to the Internet, up to multiple times daily. Customers can also choose to manually check for updates at any time.  **What is the Microsoft Malware Protection Engine?** The Microsoft Malware Protection Engine, mpengine.dll, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.  **Does this update contain any additional security-related changes to functionality?** Yes. In addition to the changes that are listed for this vulnerability, this update includes defense-in-depth updates to help improve security-related features.  **Where can I find more information about Microsoft antimalware technology?** For more information, visit the [Microsoft Malware Protection Center](https://www.microsoft.com/security/portal/) website.  **Suggested Actions** **Verify that the update is installed** Customers should verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded and installed for their Microsoft antimalware products.  For more information on how to verify the version number for the Microsoft Malware Protection Engine that your software is currently using, see the section, "Verifying Update Installation", in [Microsoft Knowledge Base Article 2510781](https://support.microsoft.com/kb/2510781).  For affected software, verify that the Microsoft Malware Protection Engine version is 1.1.14700.5 or later.  **If necessary, install the update** Administrators of enterprise antimalware deployments should ensure that their update management software is configured to automatically approve and distribute engine updates and new malware definitions. Enterprise administrators should also verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded, approved and deployed in their environment.  For end-users, the affected software provides built-in mechanisms for the automatic detection and deployment of this update. For these customers, the update will be applied within 48 hours of its availability. The exact time frame depends on the software used, Internet connection, and infrastructure configuration.  End users that do not wish to wait can manually update their antimalware software.  For more information on how to manually update the Microsoft Malware Protection Engine and malware definitions, refer to [Microsoft Knowledge Base Article 2510781](https://support.microsoft.com/kb/2510781).  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/03/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0986** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Security Essentials |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft System Center 2012 Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Intune Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft Exchange Server 2013 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft Exchange Server 2016 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft Forefront Endpoint Protection 2010 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft System Center Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Microsoft System Center 2012 R2 Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 7 for 32-bit Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 7 for x64-based Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2012 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2012 (Server Core installation) |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 8.1 for 32-bit systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 8.1 for x64-based systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2012 R2 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows RT 8.1 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2012 R2 (Server Core installation) |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1511 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1511 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2016 |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1607 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1607 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server 2016 (Server Core installation) |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1703 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1703 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1709 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows 10 Version 1709 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |
| Windows Defender on Windows Server, version 1709 (Server Core Installation) |  | Critical | Remote Code Execution |  | Base: N/A Temporal: N/A Vector: N/A |  |

# CVE-2018-0987 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0987 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0987) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0987) | **CVE Title:** Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Internet Explorer. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by changing how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Low | Information Disclosure |

## Affected Software

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

| **CVE-2018-0987** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | 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 |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | 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 |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | 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 |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | 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 |
| Internet Explorer 11 on Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | 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 |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 |
| Internet Explorer 11 on Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Low | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | 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 |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 |
| Internet Explorer 10 on Windows Server 2012 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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-2018-0988 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0988 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0988) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0988) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0988** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0989 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0989 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0989) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0989) | **CVE Title:** Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure 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 provide an attacker with information to further compromise the user's computer or data.  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. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Low | Information Disclosure |

## Affected Software

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

| **CVE-2018-0989** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Information Disclosure | 4089187 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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 | 4093114 Monthly Rollup | Important | Information Disclosure | 4088876 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Information Disclosure | 4088779 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Low | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Information Disclosure | 4089187 | 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-2018-0990 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0990 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0990) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0990) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0990** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-0991 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0991 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0991) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0991) | **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    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0991** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 |
| Internet Explorer 11 on Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 |
| Internet Explorer 11 on Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | 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 |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 |
| Internet Explorer 11 on Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 |
| Internet Explorer 10 on Windows Server 2012 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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-2018-0993 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0993 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0993) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0993) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0993** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-0994 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0994 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0994) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0994) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0994** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-0995 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0995 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0995) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0995) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0995** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-0996 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0996 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0996) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0996) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0996** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0997 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0997 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0997) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0997) | **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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-0997** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | 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 | 4093114 Monthly Rollup | Important | Remote Code Execution | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Low | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Remote Code Execution | 4088776 | 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-2018-0998 - Microsoft Edge Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0998 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0998) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0998) | **CVE Title:** Microsoft Edge Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Microsoft Edge PDF Reader 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 that contains malicious PDF content. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted PDF content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by modifying how Microsoft Edge PDF Reader handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-0998** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Low | Information Disclosure | 4088787 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Information Disclosure | 4088787 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Information Disclosure | 4088782 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Information Disclosure | 4088776 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O | Yes |

# CVE-2018-1000 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1000 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1000) | **CVE Title:** Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure 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 provide an attacker with information to further compromise the user's computer or data.  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. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Moderate | Information Disclosure |

## Affected Software

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

| **CVE-2018-1000** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Information Disclosure | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | 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 | 4093114 Monthly Rollup | Critical | Information Disclosure | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Information Disclosure | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Information Disclosure | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Information Disclosure | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Information Disclosure | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Information Disclosure | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Information Disclosure | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Information Disclosure | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Information Disclosure | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Information Disclosure | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Information Disclosure | 4088776 | 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 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Information Disclosure | 4089187 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1001 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1001 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1001) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1001) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1001** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | 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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Important | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | 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 | 4093114 Monthly Rollup | Important | Remote Code Execution | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Low | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Remote Code Execution | 4088776 | 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 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Low | Remote Code Execution | 4089187 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1003 - Microsoft JET Database Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1003 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1003) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1003) | **CVE Title:** Microsoft JET Database Engine Remote Code Execution Vulnerability  **Description:**  A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system. An attacker who successfully exploited this 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. 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.  To exploit the vulnerability, a user must open or preview a specially crafted Excel file while using an affected version of Microsoft Windows. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted Excel file to the user, and then convincing the user to open the file.  The security update addresses the vulnerability by modifying how the Microsoft JET Database Engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1003** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Remote Code Execution | 4088875 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Remote Code Execution | 4088875 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Remote Code Execution | 4088875 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Remote Code Execution | 4088875 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Remote Code Execution | 4088875 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Remote Code Execution | 4088875 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Remote Code Execution | 4088877 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Remote Code Execution | 4088877 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Remote Code Execution | 4088876 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Remote Code Execution | 4088876 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Remote Code Execution | 4088876 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Important | Remote Code Execution | 4088876 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Remote Code Execution | 4088876 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Remote Code Execution | 4088786 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Remote Code Execution | 4088786 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Remote Code Execution | 4088779 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Remote Code Execution | 4088779 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Remote Code Execution | 4088787 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Remote Code Execution | 4088782 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Remote Code Execution | 4088782 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Remote Code Execution | 4088776 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Remote Code Execution | 4088776 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Remote Code Execution | 4088776 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Remote Code Execution | 4088776 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Remote Code Execution | 4088776 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1004 - Windows VBScript Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1004 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1004) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1004) | **CVE Title:** Windows VBScript Engine Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1004** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2018-1005 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1005 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1005) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1005) | **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    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1005** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4018336 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9cf1a58c-6ac6-4d23-8492-1b15bd76d099) | Important | Elevation of Privilege | 4018293 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4018342 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c0dfd1dc-a9c2-4d25-876f-2209adc7f0ec) | Important | Elevation of Privilege | 4018298 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1007 - Microsoft Office Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1007 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1007) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1007) | **CVE Title:** Microsoft Office Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Microsoft Office 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 functions handle objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-1007** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2016 (32-bit edition) | [4011628 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5e93a303-905a-4db2-9c15-9d46c15ddcea) | Important | Information Disclosure | 3203474 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4011628 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=7df7003e-554c-4b22-b0d7-11cb3b40dceb) | Important | Information Disclosure | 3203474 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1008 - OpenType Font Driver Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1008 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1008) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1008) | **CVE Title:** OpenType Font Driver Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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.  To exploit the vulnerability, an attacker would first have to log on to a target system and then run a specially crafted application.  The security update addresses the vulnerability by correcting how ATMFD.dll handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1008** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Elevation of Privilege | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Elevation of Privilege | 4088875 | 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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Elevation of Privilege | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Elevation of Privilege | 4088875 | 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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Important | Elevation of Privilege | 4088875 | 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) | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Elevation of Privilege | 4088875 | 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 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Elevation of Privilege | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Elevation of Privilege | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | 4093114 Monthly Rollup | Important | Elevation of Privilege | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Elevation of Privilege | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Elevation of Privilege | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Elevation of Privilege | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Elevation of Privilege | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Elevation of Privilege | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Elevation of Privilege | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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 | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Elevation of Privilege | 4088776 | 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 | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Elevation of Privilege | 4088776 | 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) | [4093257 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093257) | Important | Elevation of Privilege | 4088776 | 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-2018-1009 - Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1009 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1009) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1009) | **CVE Title:** Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Windows improperly handles objects in memory and incorrectly maps kernel memory. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control over the affected system.  An attacker who successfully exploited this vulnerability could run processes in an elevated context.  The update addresses the vulnerability by correcting the way the Microsoft DirectX graphics kernel subsystem (dxgkrnl.sys) handles certain calls and escapes, to preclude improper memory mapping and to prevent unintended elevation from user mode.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1009** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Elevation of Privilege | 4088877 | 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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Important | Elevation of Privilege | 4088877 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | 4093114 Monthly Rollup | Important | Elevation of Privilege | 4088876 | 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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Important | Elevation of Privilege | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Elevation of Privilege | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Important | Elevation of Privilege | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Elevation of Privilege | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Important | Elevation of Privilege | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Important | Elevation of Privilege | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Elevation of Privilege | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Important | Elevation of Privilege | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Important | Elevation of Privilege | 4088776 | 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-2018-1010 - Microsoft Graphics Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1010 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1010) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1010) | **CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit the vulnerability:   * In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. * In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file.   The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1010** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1011 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1011 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1011) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1011) | **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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1011** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=70ec98c7-1510-4064-b4a3-6fb6a6ffe203) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0a81ef86-07cf-40dc-9eb4-fd9ac7a269eb) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | [4018350 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=2bd46d0c-df24-4428-9c8b-d7665a312ba8) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | [4018350 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=71bcf94e-f6c7-4d17-a9dc-6bc2aa49fb2c) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4018350 Security Update | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1012 - Microsoft Graphics Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1012 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1012) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1012) | **CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit the vulnerability:   * In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. * In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file.   The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1012** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1013 - Microsoft Graphics Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1013 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1013) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1013) | **CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit the vulnerability:   * In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. * In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file.   The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1013** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1014 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1014 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1014) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1014) | **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 URL to a user of an affected SharePoint server.  An attacker who successfully exploited the vulnerability could redirect users who are trying to access Silverlight content on an affected SharePoint server to malicious content if the targeted user does not already have Silverlight installed. This vulnerability requires that the user does not have Silverlight installed, clicks the specially crafted URL from the attacker, and clicks the link provided on SharePoint page to download Silverlight.  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    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1014** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4018336 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9cf1a58c-6ac6-4d23-8492-1b15bd76d099) | Important | Elevation of Privilege | 4018293 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4018342 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c0dfd1dc-a9c2-4d25-876f-2209adc7f0ec) | Important | Elevation of Privilege | 4018298 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1015 - Microsoft Graphics Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1015 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1015) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1015) | **CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit the vulnerability:   * In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. * In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file.   The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1015** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1016 - Microsoft Graphics Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1016 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1016) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1016) | **CVE Title:** Microsoft Graphics Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit the vulnerability:   * In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or instant message that takes users to the attacker's website, or by opening an attachment sent through email. * In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince users to open the document file.   The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1016** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Critical | Remote Code Execution | 4088875 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Critical | Remote Code Execution | 4088877 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Critical | Remote Code Execution | 4088876 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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 | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/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) | [4093223 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093223) | Critical | Remote Code Execution | 4056941 | Base: 8.4 Temporal: 7.6 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-1018 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1018 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1018) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1018) | **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    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1018** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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-2018-1019 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1019 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1019) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1019) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1019** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-1020 - Internet Explorer Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1020 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1020) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1020) | **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    04/10/2018 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1020** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Critical | Remote Code Execution | 4089187 | 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 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4093114 Monthly Rollup | Critical | Remote Code Execution | 4088876 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) [4092946 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4092946) | Moderate | Remote Code Execution | 4089187 | 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 | Yes |

# CVE-2018-1023 - Microsoft Browser Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1023 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1023) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1023) | **CVE Title:** Microsoft Browser Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow 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, 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 that is designed to exploit the vulnerability through Microsoft browsers, 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. 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 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 Microsoft browsers handle objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1023** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Critical | Remote Code Execution | 4088786 | 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 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Critical | Remote Code Execution | 4088779 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Critical | Remote Code Execution | 4088787 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Critical | Remote Code Execution | 4088782 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Critical | Remote Code Execution | 4088776 | 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 Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.3) | Critical | Remote Code Execution | 4088776 | 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-2018-1026 - Microsoft Office Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1026 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1026) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1026) | **CVE Title:** Microsoft Office Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in Microsoft Office 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 Office. 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 Office 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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1026** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4018288 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9caf7486-5c72-4cea-8549-6ad9bda1fe24) | Important | Remote Code Execution | 4011277 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4018288 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c2cfa971-533b-41d1-a1d5-89bd4dd41800) | Important | Remote Code Execution | 4011277 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4018288 Security Update | Important | Remote Code Execution | 4011277 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4018319 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c8f967e7-6f29-4c1d-b9a8-baf188ac56ab) | Important | Remote Code Execution | 4011095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4018319 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=7a7c41b5-df1d-40e8-b075-f0a07c40720b) | Important | Remote Code Execution | 4011095 | 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 | 4011095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4011095 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-1027 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1027 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1027) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1027) | **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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1027** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2007 Service Pack 3 | [4018353 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=736c1ece-333f-480f-9a55-3e757fb85765) | Important | Remote Code Execution | 4011714 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=70ec98c7-1510-4064-b4a3-6fb6a6ffe203) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0a81ef86-07cf-40dc-9eb4-fd9ac7a269eb) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | [4018350 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=2bd46d0c-df24-4428-9c8b-d7665a312ba8) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | [4018350 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=71bcf94e-f6c7-4d17-a9dc-6bc2aa49fb2c) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4018350 Security Update | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Compatibility Pack Service Pack 3 | [4011717 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c5de1a79-d90b-4960-982a-464ceb98869c) | Important | Remote Code Execution | 4011605 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1028 - Microsoft Office Graphics Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1028 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1028) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1028) | **CVE Title:** Microsoft Office Graphics Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when the Office graphics component improperly handles specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  There are multiple ways an attacker could exploit this vulnerability. In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit the vulnerability and then convince a user to view the website. 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 getting the user to click a link in an email or instant message that takes the user to the attacker's website, or by opening an attachment sent through email.  In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability and then convince a user to open the document file.  Note that the Preview Pane is not an attack vector for this vulnerability.  The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts.  **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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1028** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4018311 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f75ce659-9db6-432a-9f17-f0d08449ec8d) | Important | Remote Code Execution | 4011707 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4018311 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=33295029-589a-457a-aaf7-6e0a7eeed103) | Important | Remote Code Execution | 4011707 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps 2010 Service Pack 2 | [4018360 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=807ebe85-c18e-4562-859d-b967e71ab198) | Important | Remote Code Execution | 4011709 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4018330 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d1ee6f8d-a410-41f8-93e9-1ca8658e1a47) | Important | Remote Code Execution | 4011690 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4018330 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=449d39a7-633e-4e49-b736-8d41f879e9d8) | Important | Remote Code Execution | 4011690 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4018330 Security Update | Important | Remote Code Execution | 4011690 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Server 2013 Service Pack 1 | [4011586 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=07293804-dcec-4055-b5e2-d88c3cc7aa0f) | Important | Remote Code Execution | 3213560 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps Server 2013 Service Pack 1 | [4018344 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=96213651-7d4b-43fc-baae-f35d44ddab3c) | Important | Remote Code Execution | 4011692 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4018328 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=2138c5a1-561e-4593-94b7-ef4506714c61) | Important | Remote Code Execution | 4011686 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4018328 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=25de9a29-0654-4be3-8066-f83f9f79ceae) | Important | Remote Code Execution | 4011686 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018336 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9cf1a58c-6ac6-4d23-8492-1b15bd76d099) | Important | Remote Code Execution | 4018293 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Excel Services on Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4018343 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=77c62bb1-bcef-4871-8836-c0c52fddaa33) | Important | Remote Code Execution | 3213559 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 2 | [4018356 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c1912f77-fcf6-4316-93cb-a60866e2c5be) | Important | Remote Code Execution | 4011705 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Word Automation Services on Microsoft SharePoint Server 2013 Service Pack 1 | [4018341 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=a059f73f-f90e-46f0-a90d-c284a0753c82) | Important | Remote Code Execution | 4011688 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1029 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1029 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1029) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1029) | **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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1029** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2007 Service Pack 3 | [4018353 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=736c1ece-333f-480f-9a55-3e757fb85765) | Important | Remote Code Execution | 4011714 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel Viewer 2007 Service Pack 3 | [4011719 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5a52342a-a223-4bf5-bb9c-ec8a88affca1) | Important | Remote Code Execution | 4011606 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=70ec98c7-1510-4064-b4a3-6fb6a6ffe203) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4018362 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0a81ef86-07cf-40dc-9eb4-fd9ac7a269eb) | Important | Remote Code Execution | 4011675 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | [4018350 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=2bd46d0c-df24-4428-9c8b-d7665a312ba8) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | [4018350 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=71bcf94e-f6c7-4d17-a9dc-6bc2aa49fb2c) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4018350 Security Update | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac | [Release Notes Security Update](https://go.microsoft.com/fwlink/p/?linkid=831049) | Important | Remote Code Execution | 4018291 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Excel 2016 (32-bit edition) | [4018337 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c6f2ef95-8d76-46c1-817e-05aa28999905) | Important | Remote Code Execution | 4011727 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | [4018337 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=27c19300-afe4-467b-8124-4004c975f1d7) | Important | Remote Code Execution | 4011727 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4011727 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4011727 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office Compatibility Pack Service Pack 3 | [4011717 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c5de1a79-d90b-4960-982a-464ceb98869c) | Important | Remote Code Execution | 4011605 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1030 - Microsoft Office Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1030 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1030) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1030) | **CVE Title:** Microsoft Office Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in Microsoft Office 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 Office. 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 Office 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    04/10/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2018-1030** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4018288 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9caf7486-5c72-4cea-8549-6ad9bda1fe24) | Important | Remote Code Execution | 4011277 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4018288 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c2cfa971-533b-41d1-a1d5-89bd4dd41800) | Important | Remote Code Execution | 4011277 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4018288 Security Update | Important | Remote Code Execution | 4011277 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (32-bit edition) | [4018319 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c8f967e7-6f29-4c1d-b9a8-baf188ac56ab) | Important | Remote Code Execution | 4011095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4018319 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=7a7c41b5-df1d-40e8-b075-f0a07c40720b) | Important | Remote Code Execution | 4011095 | 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 | 4011095 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 4011095 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-1032 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1032 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1032) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1032) | **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    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1032** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Server 2010 Service Pack 2 | [4011712 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=a1e7b543-d5fa-4b0b-a49a-9fc96b69ad92) | Important | Elevation of Privilege | 3114998 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018336 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9cf1a58c-6ac6-4d23-8492-1b15bd76d099) | Important | Elevation of Privilege | 4018293 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4018342 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c0dfd1dc-a9c2-4d25-876f-2209adc7f0ec) | Important | Elevation of Privilege | 4018298 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1034 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1034 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1034) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1034) | **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    04/10/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2018-1034** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4018336 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9cf1a58c-6ac6-4d23-8492-1b15bd76d099) | Important | Elevation of Privilege | 4018293 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-1037 - Microsoft Visual Studio Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-1037 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1037) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1037) | **CVE Title:** Microsoft Visual Studio Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Visual Studio improperly discloses limited contents of uninitialized memory while compiling program database (PDB) files. An attacker who took advantage of this information disclosure could view uninitialized memory from the Visual Studio instance used to compile the PDB file.  To take advantage of the vulnerability, an attacker would require access to an affected PDB file created using a vulnerable version of Visual Studio. An attacker would have no way to force a developer to produce this information disclosure.  The security update addresses the vulnerability by correcting how PDB files are generated when a project is compiled.  **FAQ:**  **In addition to installing this update, are there any further steps I need to carry out to be protected from the vulnerability discussed in this CVE?** Visual Studio users who have installed the update for CVE-2018-1037 may also need to rebuild any PDB files that were updated after their initial creation, as they may contain memory leaked from the source computer used to compile Visual Studio projects. This can be done through Visual Studio after installing the applicable update or by running the standalone PDBCopy tool provided by Microsoft (see links in the table below). This tool has been updated to identify and remediate affected PDB files. Note that any projects compiled and then updated through a Visual Studio installation that has not been updated will be susceptible to memory leaks in PDB files.  **How will I know which PDB files are affected by this vulnerability?** The PDBCopy tool has been updated to assist developers in scanning for and updating affected PDB files. The tool and instructions for use can be found in [KB4131751](https://support.microsoft.com/en-us/help/4131751) with direct download links here:   | **Architecture** | **Link** | | --- | --- | | X64 | [PDBCopy.exe](https://download.visualstudio.microsoft.com/download/pr/12047014/24cf45fb80fda294721a32ce4d5224f1/pdbcopy.exe) | | X86 | [PDBCopy.exe](https://download.visualstudio.microsoft.com/download/pr/12046813/aee56c81ad71e0d9ffbd7a1feb80f2e8/pdbcopy.exe) |   **What information is leaked in PDB files compiled with a vulnerable instance of Visual Studio?** The memory leaked is limited to typically low-risk variables used in the application build environment, and only information that the Visual Studio executable uses when compiling projects. If your PDB/symbol files are shared publicly, this information could be extracted.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. Microsoft Visual Studio 2012 Update 4 and Microsoft Visual Studio 2017 Version 15.7 Preview are not yet available. This information will be updated as these security updates become available. | Important | Information Disclosure |

## Affected Software

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

| **CVE-2018-1037** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Visual Studio 2010 Service Pack 1 | [4091346 Security Update](https://download.visualstudio.microsoft.com/download/pr/12043046/0cc279e34958fb236c6005a6ffdb40dc/VS10SP1-KB4091346-x86.exe) | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2012 Update 5 | 4089501 Security Update | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2013 Update 5 | [4089283 Security Update](https://download.visualstudio.microsoft.com/download/pr/12043024/f01e9b509ff587f983ebd58ffaf435db/VS12-KB4089283.exe) | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2015 Update 3 | [4087371 Security Update](https://download.visualstudio.microsoft.com/download/pr/12043007/da90565370532f6d2ddbea5ce0303fe9/VS14-KB4087371.exe) | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2017 | [Release Notes Security Update](https://my.visualstudio.com/Downloads?q=Visual%20Studio%202017) | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2017 Version 15.7 Preview | Release Notes Security Update | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Visual Studio 2017 Version 15.6.6 | [Release Notes Security Update](https://www.visualstudio.com/downloads) | Important | Information Disclosure |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-8116 - Microsoft Graphics Component Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8116 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8116) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8116) | **CVE Title:** Microsoft Graphics Component Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists in the way that Windows handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target 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.  The security update addresses the vulnerability by correcting how Windows handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Moderate | Denial of Service |

## Affected Software

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

| **CVE-2018-8116** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Moderate | Denial of Service | 4088875 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Moderate | Denial of Service | 4088875 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Moderate | Denial of Service | 4088875 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Moderate | Denial of Service | 4088875 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4093108 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093108) [4093118 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093118) | Moderate | Denial of Service | 4088875 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4093224 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093224) | Moderate | Denial of Service | 4089344 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Moderate | Denial of Service | 4088877 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 (Server Core installation) | [4093122 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093122) [4093123 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093123) | Moderate | Denial of Service | 4088877 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 8.1 for 32-bit systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Moderate | Denial of Service | 4088876 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 8.1 for x64-based systems | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Moderate | Denial of Service | 4088876 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 R2 | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Moderate | Denial of Service | 4088876 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows RT 8.1 | 4093114 Monthly Rollup | Moderate | Denial of Service | 4088876 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4093114 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093114) [4093115 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093115) | Moderate | Denial of Service | 4088876 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 for 32-bit Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Moderate | Denial of Service | 4088786 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 for x64-based Systems | [4093111 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093111) | Moderate | Denial of Service | 4088786 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Moderate | Denial of Service | 4088779 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4093109 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093109) | Moderate | Denial of Service | 4088779 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2016 | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Denial of Service | 4088787 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Denial of Service | 4088787 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Denial of Service | 4088787 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2016 (Server Core installation) | [4093119 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093119) | Moderate | Denial of Service | 4088787 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Moderate | Denial of Service | 4088782 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4093107 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093107) | Moderate | Denial of Service | 4088782 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Moderate | Denial of Service | 4088776 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Moderate | Denial of Service | 4088776 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4093112 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093112) | Moderate | Denial of Service | 4088776 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4093224 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093224) | Moderate | Denial of Service | 4074603 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4093224 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093224) | Moderate | Denial of Service | 4089344 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4093224 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093224) | Moderate | Denial of Service | 4089344 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4093224 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4093224) | Moderate | Denial of Service | 4089344 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2018-8117 - Microsoft Wireless Keyboard 850 Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-8117 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8117) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8117) | **CVE Title:** Microsoft Wireless Keyboard 850 Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in the Microsoft Wireless Keyboard 850 which could allow an attacker to reuse an AES encryption key to send keystrokes to other keyboard devices or to read keystrokes sent by other keyboards for the affected devices. An attacker would first have to extract the AES encryption key from the affected keyboard device. The attacker would also need to maintain physical proximity â€“ within wireless range â€“ of the devices for the duration of the attack.  An attacker could use the vulnerability to inject arbitrary keyboard HID packets into a keyboard's dongle. For example, an attacker could simulate keystrokes to send malicious commands into a victim's computer. An attacker could also read keystrokes such as passwords sent by other keyboards for the affected devices.  The update enhances security by mandating unique AES encryption keys are generated for each wireless keyboard device.  **FAQ:**  **1. What do I need to download and install to be protected from this vulnerability?**   1. Click the "Security Update link" in the **Affected Products** table. 2. On the Wireless Keyboard 850 page, scroll down to the **Downloads** list. 3. Under Software and Drivers, select the operating system and architecture for your system. 4. Click **Wireless Keyboard 850 Update**. 5. Click **Run**.   Note that you do not have to restart your system after installing the update.  **2. After I installed the update, my keyboard stopped responding. What do I do?**  If after installing the update your keyboard stops responding, remove and re-insert the batteries to reset your keyboard.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    04/10/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2018-8117** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Wireless Keyboard 850 | [Information Security Update](https://go.microsoft.com/fwlink/?linkid=871281) | Important | Security Feature Bypass |  | Base: N/A Temporal: N/A Vector: N/A | No |

**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