微软发布 5 月补丁修复 82 个安全问题

安全威胁通告

发布时间：2019 年 5 月 15 日

综述

微软于周二发布了 5 月安全更新补丁，修复了 82 个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及.NET Core、.NET Framework、Adobe Flash Player、Azure、Internet Explorer、Kerberos、Microsoft Browsers、Microsoft Dynamics、Microsoft Edge、Microsoft Graphics Component、Microsoft JET Database Engine、Microsoft Office、Microsoft Office SharePoint、Microsoft Scripting Engine、Microsoft Windows、NuGet、Servicing Stack Updates、Skype for Android、SQL Server、Team Foundation Server、Windows DHCP Server、Windows Diagnostic Hub、Windows Kernel、Windows NDIS 以及 Windows RDP。

相关信息如下：

产品	CVE 编号	CVE 标题	严重程度
.NET Core	CVE-2019-0980	.Net Framework and .Net Core 拒绝服务漏洞	Important
.NET Core	CVE-2019-0981	.Net Framework and .Net Core 拒绝服务漏洞	Important
.NET Core	CVE-2019-0982	ASP.NET Core 拒绝服务漏洞	Important
.NET Framework	CVE-2019-0820	.NET Framework and .NET Core 拒绝服务漏洞	Important
.NET Framework	CVE-2019-0864	.NET Framework 拒绝服务漏洞	Important
Adobe Flash Player	ADV190012	May 2019 Adobe Flash 安全更新	Critical

Azure	CVE-2019-1000	Microsoft Azure AD Connect 特权提升漏洞	Important
Internet Explorer	CVE-2019-0921	Internet Explorer 欺骗漏洞	Important
Internet Explorer	CVE-2019-0929	Internet Explorer 内存破坏漏洞	Critical
Internet Explorer	CVE-2019-0930	Internet Explorer 信息泄露漏洞	Important
Internet Explorer	CVE-2019-0995	Internet Explorer 安全功能绕过漏洞	Important
Kerberos	CVE-2019-0734	Windows 特权提升漏洞	Important
Microsoft Browsers	CVE-2019-0940	Microsoft Browser 内存破坏漏洞	Critical

Microsoft Dynamics	CVE-2019-1008	Microsoft Dynamics On-Premise Security Feature Bypass	Important
Microsoft Edge	CVE-2019-0926	Microsoft Edge 内存破坏漏洞	Critical
Microsoft Edge	CVE-2019-0938	Microsoft Edge 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2019-0882	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-0892	Win32k 特权提升漏洞	Important
Microsoft Graphics Component	CVE-2019-0903	GDI+ 远程代码执行漏洞	Critical
Microsoft Graphics Component	CVE-2019-0961	Windows GDI 信息泄露漏洞	Important
Microsoft Graphics Component	CVE-2019-0758	Windows GDI 信息泄露漏洞	Important

Microsoft JET Database Engine	CVE-2019-0893	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0894	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0895	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0896	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0897	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0898	Jet Database Engine 远程代码执行漏洞	Important

Microsoft JET Database Engine	CVE-2019-0899	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0900	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0901	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0902	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0889	Jet Database Engine 远程代码执行漏洞	Important
Microsoft JET Database Engine	CVE-2019-0890	Jet Database Engine 远程代码执行漏洞	Important

Microsoft JET Database Engine	CVE-2019-0891	Jet Database Engine 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-0945	Microsoft Office Access Connectivity Engine 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-0946	Microsoft Office Access Connectivity Engine 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-0947	Microsoft Office Access Connectivity Engine 远程代码执行漏洞	Important
Microsoft Office	CVE-2019-0953	Microsoft Word 远程代码执行漏洞	Critical

Microsoft Office SharePoint	CVE-2019-0956	Microsoft SharePoint Server 信息泄露漏洞	Important
Microsoft Office SharePoint	CVE-2019-0957	Microsoft SharePoint 特权提升漏洞	Important
Microsoft Office SharePoint	CVE-2019-0958	Microsoft SharePoint 特权提升漏洞	Important
Microsoft Office SharePoint	CVE-2019-0963	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-0949	Microsoft SharePoint 欺骗漏洞	Important
Microsoft Office SharePoint	CVE-2019-0950	Microsoft SharePoint 欺骗漏洞	Important
Microsoft Office SharePoint	CVE-2019-0951	Microsoft SharePoint 欺骗漏洞	Important

Microsoft Office SharePoint	CVE-2019-0952	Microsoft SharePoint Server 远程代码执行漏洞	Important
Microsoft Scripting Engine	CVE-2019-0884	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0911	Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0912	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0913	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0914	Chakra Scripting Engine 内存破坏漏洞	Moderate

Microsoft Scripting Engine	CVE-2019-0915	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0916	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0917	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0918	Scripting Engine 内存破坏漏洞	Moderate
Microsoft Scripting Engine	CVE-2019-0922	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0923	Chakra Scripting Engine 内存破坏漏洞	Important

Microsoft Scripting Engine	CVE-2019-0924	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0925	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0927	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0933	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Scripting Engine	CVE-2019-0937	Chakra Scripting Engine 内存破坏漏洞	Critical
Microsoft Windows	CVE-2019-0863	Windows Error Reporting 特权提升漏洞	Important

Microsoft Windows	CVE-2019-0886	Windows Hyper-V 信息泄露漏洞	Important
Microsoft Windows	CVE-2019-0942	Unified Write Filter 特权提升漏洞	Important
Microsoft Windows	CVE-2019-0733	Windows Defender Application Control 安全功能绕过漏洞	Important
Microsoft Windows	CVE-2019-0885	Windows OLE 远程代码执行漏洞	Important
Microsoft Windows	CVE-2019-0931	Windows Storage Service 特权提升漏洞	Important
Microsoft Windows	ADV190013	Microsoft Guidance to mitigate Microarchitectural Data Sampling vulnerabilities	Important

Microsoft Windows	CVE-2019-0936	Windows 特权提升漏洞	Important
NuGet	CVE-2019-0976	NuGet Package Manager Tampering Vulnerability	Important
Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
Skype for Android	CVE-2019-0932	Skype for Android 信息泄露漏洞	Important
SQL Server	CVE-2019-0819	Microsoft SQL Server Analysis Services 信息泄露漏洞	Important
Team Foundation Server	CVE-2019-0971	Azure DevOps Server and Team Foundation Server 信息泄露漏洞	Important

Team Foundation Server	CVE-2019-0872	Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability	Important
Team Foundation Server	CVE-2019-0979	Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability	Important
Windows DHCP Server	CVE-2019-0725	Windows DHCP Server 远程代码执行漏洞	Critical
Windows Diagnostic Hub	CVE-2019-0727	Diagnostic Hub Standard Collector, Visual Studio Standard Collector 特权提升漏洞	Important
Windows Kernel	CVE-2019-0881	Windows Kernel 特权提升漏洞	Important
Windows NDIS	CVE-2019-0707	Windows NDIS 特权提升漏洞	Important

Windows RDP	CVE-2019-0708	Remote Desktop Services 远程代码执行漏洞	Critical

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

附件

ADV190012 - May 2019 Adobe Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190012 MITRE NVD	**CVE Title:** May 2019 Adobe Flash Security Update **Description:** This security update addresses the following vulnerability, which is described in Adobe Security Bulletin APSB19-26: CVE-2019-7837. **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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. 6. [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	7. "Compatibility Flags"=dword:00000400 8. 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 What is Group Policy Object Editor? Core Group Policy tools and settings 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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 2. Double-click the .reg file to apply it to an individual system. 3. **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. **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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

ADV190012						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows Server 2012	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for 32-bit systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190012						
Adobe Flash Player on Windows RT 8.1	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal:	Yes

ADV190012						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190012						
Adobe Flash Player on Windows 10 Version 1803 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for ARM64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for ARM64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2019	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal:	Yes

ADV190012						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1709 for ARM64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1903 for 32-bit Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1903 for x64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1903 for ARM64-based Systems	4497932 Security Update	Critical	Remote Code Execution	4493478	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190013 - Microsoft Guidance to mitigate Microarchitectural Data Sampling vulnerabilities

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190013 MITRE NVD	**CVE Title:** Microsoft Guidance to mitigate Microarchitectural Data Sampling vulnerabilities **Description:** Executive Summary On May 14, 2019, Intel published information about a new subclass of speculative execution side channel vulnerabilities known as Microarchitectural Data Sampling. An attacker who successfully exploited these vulnerabilities may be able to read privileged data across trust boundaries. In shared resource environments (such as exists in some cloud services configurations), these vulnerabilities could allow one virtual machine to improperly access information from another. In non-browsing scenarios on	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	standalone systems, an attacker would need prior access to the system or an ability to run a specially crafted application on the target system to leverage these vulnerabilities. These vulnerabilities are known as: • CVE-2018-12126 - Microarchitectural Store Buffer Data Sampling (MSBDS)â€¯ • CVE-2018-12130 - Microarchitectural Fill Buffer Data Sampling (MFBDS) • CVE-2018-12127 - Microarchitectural Load Port Data Sampling (MLPDS) • CVE-2019-11091 - Microarchitectural Data Sampling Uncacheable Memory (MDSUM) Important: These issues will affect other systems such as Android, Chrome, iOS, Linux, and MacOS. We advise customers seek to guidance from their respective vendors. Microsoft has released software updates to help mitigate these vulnerabilities. To get all available protections, firmware (microcode) and software updates are required. This may include microcode from device OEMs. In some cases, installing these updates will have a performance impact. We have also acted to secure our cloud services. Microsoft has no information to indicate that these vulnerabilities have been used to attack customers at this time. Microsoft continues working closely with industry partners including chip makers, hardware OEMs, and app vendors to protect customers.		

Recommended Actions

To protect your system from these vulnerabilities, Microsoft recommends that you take the following actions, and refer to the subsequent sections for links to further information for your specific situation:

1. The best protection is to keep computers up to date. This includes installing OS and microcode updates.

- To be fully protected, customers may also need to disable Hyper-Threading (also known as Simultaneous Multi Threading (SMT)). Please see Knowledge Base Article 4073757â€¯for guidance on protecting Windows devices.
- OEMs might also provide additional guidance. Customers using Surface products should seeâ€¯Microsoft Knowledge Base Article 4073065.

2. Microsoft recommends that enterprise customers review this advisory in detail and register for the security notifications mailer to be alerted of content changes to this advisory. Seeâ€¯Microsoft Technical Security Notifications.
3. Software developers should review the C++ developer guidance for speculative execution side channels.
4. Verify the status of protections for the various CVEs by running the PowerShell script **Get-SpeculationControlSettings**. For more information and to obtain the

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	PowerShell script seeâ€¯Understanding Get-SpeculationControlSettings PowerShell script output. **Important** Please note that at the release of this advisory, microcode updates provided by Microsoft for Intel processors are not available for the following versions of Windows. These microcode updates will be released at a later date. Microsoft recommends that customers running these versions of Windows install applicable Windows updates and obtain microcode updates for Intel-based devices from their OEM:: • Windows 10 Version 1803 for x64-based Systems • Windows Server, version 1803 (Server Core Installation) • Windows 10 Version 1809 for x64-based Systems • Windows Server 2019 • Windows Server 2019 (Server Core installation) # Microsoft Windows client customers Customers using Windows client operating systems need to apply both firmware (microcode) and software updates. Seeâ€¯Microsoft Knowledge Base Article 4073119â€¯ for additional information. Microsoft is making available Intel-validated microcode		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	updates for Windows 10 operating systems. Please seeâ€¯Microsoft Knowledge Base Article 4093836â€¯ for the current Intel microcode updates. In addition, customers should check to see if their OEM is providing additional guidance on updates and mitigations. Surface Support Article 4073065 provides more information to Surface customers. Microsoft Windows Server customers Customers using Windows server operating systems listed in theâ€¯Affected Productsâ€¯table need to apply firmware (microcode) and software updates as well as to configure protections. Seeâ€¯Microsoft Knowledge Base Article 4072698â€¯for additional information, including workarounds. Microsoft Azure has taken steps to address the security vulnerabilities at the hypervisor level to protect Windows Server VMs running in Azure. More information can be foundâ€¯here.		

Microsoft cloud customers

Microsoft has already deployed mitigations across our cloud services. More information is availableâ€¯here.

Microsoft SQL Server customers

In scenarios running Microsoft SQL Server, customers should follow the guidance outlined inâ€¯Microsoft Knowledge Base Article 4073225.

Microsoft HoloLens customers

Updates to Windows 10 for HoloLens are available to HoloLens customers through Windows Update.

Afterâ€¯applyingâ€¯theâ€¯February 2018 Windows Security Updateâ€¯HoloLens customers do not need to take any additional action to update their device firmware. These mitigations will also be included in all future releases of Windows 10 for HoloLens.

Potential performance impacts

Specific performance impact varies by hardware generation and implementation by the chip manufacturer. For most consumer devices, impact on performance may not be noticeable. Some customers may have to disable Hyper-Threading (SMT) to fully address the risk from MDS vulnerabilities. In testing Microsoft has seen some performance impact with these mitigations, in particular when hyperthreading is disabled. Microsoft values the security of its software and services and has made the decision to implement certain mitigation strategies in an effort to better secure our products. In some cases, mitigations are not enabled by default to allow users and administrators to evaluate the performance impact and risk exposure before deciding to enable the mitigations. We continue to work with hardware vendors to improve performance while maintaining a high level of security.

References

See the following for further information from Intel:

- Intel Security advisory (Intel-SA-00233): https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• Software Security Guidance for developers: https://software.intel.com/security-software-guidance/software-guidance/microarchitectural-data-sampling • MDS: https://www.intel.com/content/www/us/en/architecture-and-technology/mds.html • www.intel.com/securityfirst FAQ **1. When will the firmware updates be available?** If you have a non-Microsoft device, we suggest contacting your OEM for this information. **2. Will there be updates for Windows operating systems?** Yes. Please see the Security Updates table. **3. I am running Windows Server 2008 for x64-based Systems. Is an update available for my system?** At the time of release, an update is not available for Windows Server 2008 for x64-based Systems. When the update is available, customers will be notified through a revision to this advisory. If you wish to be notified when the update is released, Microsoft		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	recommends that you register for the security notifications mailer to be alerted of content changes to this advisory. Seeâ€¯Microsoft Technical Security Notifications. **4. Where can I find information regarding other speculative side-channel execution vulnerabilities?** • For information on Microsoft guidance for Spectre and Meltdown vulnerabilities, see â€¯ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities. • For information about Microsoft guidance for CVE-2018-3639, seeâ€¯ADV180012 | Microsoft Guidance for Speculative Store Bypass. • For information about Microsoft guidance for CVE-2018-3640, see ADV180013 | Microsoft Guidance for Rogue System Register Read • For information about Microsoft guidance for L1 Terminal Fault vulnerabilities, see ADV180018 | Microsoft Guidance to mitigate L1TF variant **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

ADV190013						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190013						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Information Disclosure	4493451	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Information Disclosure	4493451	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165	Important	Information Disclosure	4493446	Base: N/A Temporal:	Yes

ADV190013						
	Security Only				N/A Vector: N/A	
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Information Disclosure	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4494440 Security Update	Important	Information Disclosure	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security	Important	Information Disclosure	4493470	Base: N/A Temporal:	Yes

ADV190013						
	Update				N/A Vector: N/A	
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Information Disclosure	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Information Disclosure	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Information Disclosure	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190013						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4494441 Security Update	Important	Information Disclosure	4493509	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Information Disclosure	4493509	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Information Disclosure	4493509	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Information Disclosure	4493509	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001 - Latest Servicing Stack Updates

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV990001 MITRE NVD	**CVE Title:** Latest Servicing Stack Updates **Description:** This is a list of the latest servicing stack updates for each operating sytem. This list will be updated whenever a new servicing stack update is released. It is important to install the latest servicing stack update. **FAQ:** **1. Why are all of the Servicing Stack Updates (SSU) critical updates?** The SSUs are classified as Critical updates. This does not indicate that there is a critical vulnerability being addressed in the update. **2. When was the most recent SSU released for each version of Microsoft Windows?** Please refer to the following table for the most recent SSU release. We will update the entries any time a new SSU is released:	Critical	Defense in Depth

CVE ID	Vulnerability Description			Maximum Severity Rating	Vulnerability Impact
	Product	**SSU Package**	**Date Released**		
	Windows Server 2008	4493730	April 2019		
	Windows 7/Server 2008 R2	4490628	March 2019		
	Windows Server 2012	3173426	July 2016		
	Windows 8.1/Server 2012 R2	3173424	July 2016		
	Windows 10	4498353	May 2019		
	Windows 10 Version 1607/Server 2016	4498947	May 2019		
	Windows 10 Version 1703	4500640	May 2019		
	Windows 10 1709/Windows Server, version 1709	4500641	May 2019		
	Windows 10 1803/Windows Server, version 1803	4497398	May 2019		
	Windows 10 1809/Server 2019	4499728	May 2019		
	Windows 10 1903/Windows Server, version 1903	4500109	May 2019		
	Mitigations: None **Workarounds:** None				

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/13/2018 08:00:00 Information published. 1.1 11/14/2018 08:00:00 Corrected the link to the Windows Server 2008 Servicing Stack Update. This is an informational change only. 5.0 02/12/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1607, Windows Server 2016, and Windows Server 2016 (Server Core installation); Windows 10 Version 1703; Windows 10 Version 1709 and Windows Server, version 1709 (Server Core Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 5.2 02/14/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1803 for x64-based Systems to 4485449. This is an informational change only. 6.0 03/12/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A Servicing Stack Update has been released for Windows 7 and Windows Server 2008 R2 and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information. 1.2 12/03/2018 08:00:00 FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only. 5.1 02/13/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1809 for x64-based Systems to 4470788. This is an informational change only. 8.0 05/14/2019 07:00:00 A Servicing Stack Update has been released for Windows 10 version 1507, Windows 10 version 1607, Windows Server 2016, Windows 10 version 1703, Windows 10 version 1709, Windows Server, version 1709, Windows 10 version 1803, Windows Server, version 1803, Windows 10 version 1809, Windows Server 2019, Windows 10 version 1809 and Windows Server, version 1809. See the FAQ section for more information. 3.2 12/12/2018 08:00:00 Fixed a typo in the FAQ.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	7.0 04/09/2019 07:00:00 A Servicing Stack Update has been released for Windows Server 2008 and Windows Server 2008 (Server Core installation); Windows 10 version 1809, Windows Server 2019, and Windows Server 2019 (Server Core installation). See the FAQ section for more information. 3.0 12/11/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 4.0 01/08/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1703. See the FAQ section for more information. 3.1 12/11/2018 08:00:00 Updated supersedence information. This is an informational change only. 2.0 12/05/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information.		

Affected Software

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

ADV990001						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	3173426 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	3173426 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2012 R2	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	3173424 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4498353 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4498353 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4498947 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1607 for 32-bit Systems	4498947 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4498947 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4498947 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4500640 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4500640 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1709 for x64-based Systems	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1709 (Server Core Installation)	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1803 for ARM64-based Systems	4497398 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for 32-bit Systems	4499728 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4499728 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4499728 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4499728 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4499728 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows 10 Version 1709 for ARM64-based Systems	4500641 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4493730 Servicing Stack Update	Critical	Defense in Depth	955430	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0707 - Windows NDIS Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0707 MITRE NVD	**CVE Title:** Windows NDIS Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it. To exploit the vulnerability, in a local attack scenario, an attacker could run a specially crafted application to elevate the attacker's privilege level. An attacker who successfully exploited this vulnerability could run processes in an elevated context. However, an attacker must first gain access to the local system with the ability to execute a malicious application in order to exploit this vulnerability. The security update addresses the vulnerability by changing how ndis.sys validates buffer length. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0707						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4499158 Security Only 4499171 Monthly	Important	Elevation of Privilege	4493451	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0707						
	Rollup					
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Elevation of Privilege	4493451	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	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	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	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0707						
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	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	4499151 Monthly Rollup	Important	Elevation of Privilege	4493446	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)	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	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	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0707						
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	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	4494440 Security Update	Important	Elevation of Privilege	4493470	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	4494440 Security Update	Important	Elevation of Privilege	4493470	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	4494440 Security Update	Important	Elevation of Privilege	4493470	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)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0707						
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	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	4499181 Security Update	Important	Elevation of Privilege	4493474	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	4499179 Security Update	Important	Elevation of Privilege	4493441	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	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4499167 Security	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3	Yes

CVE-2019-0707						
32-bit Systems	Update				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	
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4494441 Security	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3	Yes

CVE-2019-0707						
32-bit Systems	Update				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	
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0707						
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	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 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	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 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	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 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0707						
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0708 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0708 MITRE NVD	**CVE Title:** Remote Desktop ServicesÂ Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Remote Desktop Services â€" formerly known as Terminal Services â€" when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP. The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests. **FAQ:** None **Mitigations:** **Workarounds:** The following workarounds may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave these workarounds in place: **1. Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	You can enable Network Level Authentication to block unauthenticated attackers from exploiting this vulnerability. With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before the attacker could exploit the vulnerability. **2. Block TCP port 3389 at the enterprise perimeter firewall** TCP port 3389 is used to initiate a connection with the affected component. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks. However, systems could still be vulnerable to attacks from within their enterprise perimeter. **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0708						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/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	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0708						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/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	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/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	4499164 Monthly Rollup 4499175 Security	Critical	Remote Code Execution	4493472	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0708						
Service Pack 1	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/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	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/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	4499149 Monthly Rollup 4499180 Security	Critical	Remote Code Execution	4493471	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0708						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/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)	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0725 - Windows DHCP Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0725 MITRE NVD	**CVE Title:** Windows DHCP Server Remote Code Execution Vulnerability **Description:** A memory corruption vulnerability exists in the Windows Server DHCP service when processing specially crafted packets. An attacker who successfully exploited the vulnerability could run arbitrary code on the DHCP server. To exploit the vulnerability, a remote unauthenticated attacker could send a specially crafted packet to an affected DHCP server. The security update addresses the vulnerability by correcting how DHCP servers handle network packets. **FAQ:** None **Mitigations:** None **Workarounds:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0725						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0725						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly	Critical	Remote Code Execution	4493451	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0725						
	Rollup					
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Critical	Remote Code Execution	4493451	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Critical	Remote Code Execution	4493446	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Critical	Remote Code Execution	4493446	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0725						
Windows Server 2016	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server	4494441 Security	Critical	Remote Code Execution	4493509	Base: 8.1 Temporal: 7.3	Yes

CVE-2019-0725						
Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Critical	Remote Code Execution	4493509	Base: 8.1 Temporal: 7.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0727 - Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0727 MITRE NVD	**CVE Title:** Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector allows file deletion in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by not permitting Diagnostics Hub Standard Collector or the Visual Studio Standard Collector to delete files in arbitrary locations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0727						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2015 Update 3	4489639 Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0727						
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0727						
x64-based Systems						
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0727						
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0727						
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Visual	Release Notes Security	Important	Elevation of Privilege	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0727						
Studio 2017 version 15.9	Update					
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 6.7 Temporal: 6 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0727						
(Server Core installation)						
Microsoft Visual Studio 2017 version 15.0	Release Notes Security Update	Important	Elevation of Privilege	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Visual Studio 2019 version 16.0	Release Notes Security Update	Important	Elevation of Privilege	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0733 - Windows Defender Application Control Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0733 MITRE NVD	**CVE Title:** Windows Defender Application Control Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement. An attacker who successfully exploited this vulnerability could circumvent Windows PowerShell Constrained Language Mode on the machine. To exploit the vulnerability, an attacker would first have to access the local machine, and then place PowerShell into Constrained Language mode. By doing that an attacker could leverage script debugging to abuse signed modules in an unintended way. The update addresses the vulnerability by correcting how PowerShell functions in Constrained Language Mode. **FAQ:** None	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0733						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4499154 Security	Important	Security Feature Bypass	4493475	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0733						
	Update				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	
Windows 10 for x64-based Systems	4499154 Security Update	Important	Security Feature Bypass	4493475	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	4494440 Security Update	Important	Security Feature Bypass	4493470	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	4494440 Security Update	Important	Security Feature Bypass	4493470	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	4494440 Security Update	Important	Security Feature Bypass	4493470	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)	4494440 Security Update	Important	Security Feature Bypass	4493470	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0733						
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Security Feature Bypass	4493474	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	4499181 Security Update	Important	Security Feature Bypass	4493474	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	4499179 Security Update	Important	Security Feature Bypass	4493441	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	4499179 Security Update	Important	Security Feature Bypass	4493441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0733						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0733						
based Systems						
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Security Feature Bypass	4493441	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 1903	4497936 Security	Important	Security Feature Bypass	4493441	Base: 5.3 Temporal: 4.8	Yes

CVE-2019-0733						
for 32-bit Systems	Update				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	
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Security Feature Bypass	4493441	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 1903 for ARM64-based Systems	4497936 Security Update	Important	Security Feature Bypass	4493441	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 1903 (Server Core installation)	4497936 Security Update	Important	Security Feature Bypass	4493441	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0734 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0734 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully decode and replace authentication request using Kerberos, allowing an attacker to be validated as an Administrator. The update addresses this vulnerability by changing how these requests are validated. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.	Important	Elevation of Privilege

Affected Software

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

CVE-2019-0734						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Service Pack 1	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Elevation of Privilege	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly	Important	Elevation of Privilege	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
	Rollup					
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Windows RT 8.1	4499151 Monthly Rollup	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4499149 Monthly Rollup 4499180	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0734						
Service Pack 2	Security Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0758 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0758 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0758						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0758						
Systems Service Pack 1	4499175 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499158 Security Only 4499171 Monthly	Important	Information Disclosure	4493451	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
	Rollup					
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Information Disclosure	4493451	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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-	4499151 Monthly	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0758						
based systems	Rollup 4499165 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0758						
(Server Core installation)	Rollup 4499165 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Information Disclosure	4493475	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499154 Security Update	Important	Information Disclosure	4493475	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4499167 Security	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0758						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499149 Monthly Rollup 4499180 Security	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0758						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0819 - Microsoft SQL Server Analysis Services Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0819 MITRE NVD	**CVE Title:** Microsoft SQL Server Analysis Services Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft SQL Server Analysis Services when it improperly enforces metadata permissions. An attacker who successfully exploited the vulnerability could query tables or columns for which they do not have access rights. To exploit this vulnerability, an authenticated attacker would need to submit a query to an affected Analysis Services database. The security update addresses the vulnerability by correcting how SQL Server Analysis Services enforces permissions. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability relates to SQL table columns that would normally be restricted. **There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?** • First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article 321185 - How to determine the version, edition, and update level of SQL Server and its components. • Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install. **Note** If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates.		

CVE ID	Vulnerability Description				Maximum Severity Rating	Vulnerability Impact
	Update number	**Title**	**Apply if current product version isâ€¦**	**This security update also includes servicing releases up throughâ€¦**		
	4494351	Description of the security update for the Information Disclosure vulnerability in SQL Server 2017 (GDR): May 14, 2019	14.0.1000.169 - 14.0.2002.14	4293803		
	4494351	Description of the security update for the Remote Code Execution vulnerability in SQL Server 2017 (CU+GDR): May 14, 2019	14.0.3006.16 - 14.0.3076.1	KB4484710 â€“ RTM CU14		
	What are the GDR and CU update designations and how do they differ? The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different update servicing branches in place for SQL Server. The primary difference between the two is that CU branches cumulatively include all updates for a given baseline, while GDR branches include only cumulative critical updates for a given baseline. A baseline can be the initial RTM release or a Service Pack. For any given baseline, *either* the GDR or CU updates are options if you are a) at the baseline version (never installed any servicing updates, CU or GDR), or b) have only					

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	installed GDR updates. The CU update is the only option if you have installed a previous SQL Server CU for the baseline you are on. **Does this security update apply to SQL Server 2017 on Linux or on Linux Docker Containers?** No. The fix is only applicable to SQL Server Analysis Services (AS), which is not available within SQL Server 2017 on Linux. **Will these security updates be offered to SQL Server clusters?** Yes. The updates will also be offered to SQL Server 2017 RTM instances that are clustered. Updates for SQL Server clusters will require user interaction. If the SQL Server 2017 RTM cluster has a passive node, to reduce downtime, Microsoft recommends that you scan and apply the update to the inactive node first, then scan and apply it to the active node. When all components have been updated on all nodes, the update will no longer be offered. **Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?** Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0819						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0819						
Microsoft SQL Server 2017 for x64-based Systems (GDR)	4494351 Security Update	Important	Information Disclosure	4293803	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2017 for x64-based Systems (CU+GDR)	4494352 Security Update	Important	Information Disclosure	4293805	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820 - .NET Framework and .NET Core Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0820 MITRE NVD	**CVE Title:** .NET Framework and .NET Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when .NET Framework and .NET Core improperly process RegEx strings. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET application.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to a .NET Framework (or .NET core) application. The update addresses the vulnerability by correcting how .NET Framework and .NET Core applications handle RegEx string processing. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0820						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499406 Monthly Rollup	Important	Denial of Service		Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
	4498961 Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4498963 Security Only	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal:	Maybe

CVE-2019-0820						
	4499408 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal:	Maybe

CVE-2019-0820						
	4499409 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
.NET Core 1.0	Release Notes Security Update	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 1.1	Release Notes Security Update	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4499167 Security	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Yes

CVE-2019-0820						
	Update				Vector: N/A	
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4498962 Security Only 4499407 Monthly	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
	Rollup					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4498963 Security Only 4499408	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A	Yes

CVE-2019-0820						
					Vector: N/A	
.NET Core 2.1	Release Notes Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 2.2	Release Notes Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
	Rollup					
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407	Important	Denial of Service	4493470	Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4499408 Monthly	Important	Denial of Service	4493470	Base: N/A Temporal:	Maybe

CVE-2019-0820						
	Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4495610 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4495610 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4495610 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
					Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4495610 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4495611 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4495611 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4495613 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4495613 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4495616 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4495616 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4495616 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly	Important	Denial of Service	4493470	Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
	Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1903 (Server Core installation)	4495620 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
	Rollup					
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0820						
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Yes

CVE-2019-0820						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0820						
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)	4499405 Monthly	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
	Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server, version 1903 (Server Core installation)	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0820						
	Rollup					
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A	Maybe

CVE-2019-0820						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0863 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0863 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with administrator privileges. To exploit the vulnerability, an attacker must first gain unprivileged execution on a victim system. The security update addresses the vulnerability by correcting the way WER handles files. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0863						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based	4499164 Monthly Rollup 4499175 Security	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Elevation of Privilege	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly	Important	Elevation of Privilege	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
	Rollup					
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Windows RT 8.1	4499151 Monthly Rollup	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0863						
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0864 - .NET Framework Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0864	**CVE Title:** .NET Framework Denial of Service Vulnerability **Description:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A denial of service vulnerability exists when .NET Framework improperly handles objects in heap memory. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET application. 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 .NET Framework handle objects in heap memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0864						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4499406 Monthly Rollup	Important	Denial of Service		Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	4498961 Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4498962 Security Only 4499407 Monthly	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
	Rollup					
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
	Rollup					
Microsoft .NET Framework 4.6.2 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2 on Windows 10 for x64-based Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0864						
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems	4499167 Security	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Yes

CVE-2019-0864						
	Update				Vector: N/A	
Microsoft .NET Framework 4.7.2 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4498962 Security Only 4499407 Monthly	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
	Rollup					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A	Yes

CVE-2019-0864						
					Vector: N/A	
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0864						
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	4499406 Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
	Rollup					
Microsoft .NET Framework 4.8 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2016	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4495611 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4495611 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4495613 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4495613 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4495616 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	Update				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 4.8 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1903 (Server Core installation)	4495620 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4499154 Security	Important	Denial of Service	4493475	Base: N/A Temporal:	Yes

CVE-2019-0864						
	Update				N/A Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0864						
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4499179 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Yes

CVE-2019-0864						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0864						
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Yes

CVE-2019-0864						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server, version 1903 (Server Core installation)	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
	Rollup					
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0864						
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal:	Maybe

CVE-2019-0864						
	Only 4499406 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A	Maybe

CVE-2019-0864						
	Monthly Rollup				Vector: N/A	

CVE-2019-0872 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0872 MITRE NVD	**CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability **Description:** A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0872						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2017 Update 3.1	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2018 Update 1.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Azure DevOps Server 2019	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2015 Update 4.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0881 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0881 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Kernel improperly handles key enumeration. An attacker who successfully exploited the vulnerability could gain elevated privileges on a targeted system. A locally authenticated attacker could exploit this vulnerability by running a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel properly handles key enumeration. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0881						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based	4499164 Monthly Rollup	Important	Elevation of Privilege	4493472	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0881						
Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Elevation of Privilege	4493451	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Elevation of Privilege	4493451	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4499151 Monthly Rollup	Important	Elevation of Privilege	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4499167 Security	Important	Elevation of Privilege	4493464	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0881						
32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4494441 Security	Important	Elevation of Privilege	4493509	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0881						
32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0881						
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0882 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0882 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0882						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0882						
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 449917	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Service Pack 1 (Server Core installation)	5 Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499158 Security Only 4499171 Monthly Rollup	Important	Information Disclosure	4493451	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499158 Security Only	Important	Information Disclosure	4493451	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0882						
Core installation)	4499171 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Information Disclosure	4493475	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499154 Security Update	Important	Information Disclosure	4493475	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0882						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows Server 2019	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 (Server Core installation)	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499149 Monthly Rollup 449918	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Systems Service Pack 2	0 Security Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0882						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0884 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0884						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for	4499149 Monthly Rollup 4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
32-bit Systems Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	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	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	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	4498206 IE Cumulative 4499164 Monthly Rollup	Moderate	Remote Code Execution	4493472	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Internet Explorer 11 on Windows Server 2012	4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	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	4498206 IE Cumulative 4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4498206 IE Cumulative 4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Internet Explorer 11 on Windows Server 2012 R2	4498206 IE Cumulative 4499151 Monthly Rollup	Moderate	Remote Code Execution	4493446	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	4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4499154 Security Update	Critical	Remote Code Execution	4493475	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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	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	4494440 Security Update	Critical	Remote Code Execution	4493470	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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Version 1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	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-	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	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	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
10 Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Version 1709 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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 1903 for x64-	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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	4498206 IE Cumulative 4499171 Monthly Rollup	Moderate	Remote Code Execution	4493451	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
Microsoft Edge on Windows 10 for	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
32-bit Systems						
Microsoft Edge on Windows 10 for x64-based Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499167 Security	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0884						
10 Version 1803 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
ARM64-based Systems						
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0884						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0885 - Windows OLE Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0885 MITRE NVD	**CVE Title:** Windows OLE Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file or a program, causing Windows to execute arbitrary code. The update addresses the vulnerability by correcting how Windows OLE validates user input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0885						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0885						
Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4499167 Security	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7	Yes

CVE-2019-0885						
32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4494441 Security	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7	Yes

CVE-2019-0885						
32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0885						
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0886 - Windows Hyper-V Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0886 MITRE NVD	**CVE Title:** Windows 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:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Guest VM to Hyper-V host server - virtualization security boundary. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0886						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4494440 Security Update	Important	Information Disclosure	4493470	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Information Disclosure	4493470	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Information Disclosure	4493470	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Information Disclosure	4493474	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0886						
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Information Disclosure	4493464	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0886						
Windows Server 2019	4494441 Security Update	Important	Information Disclosure	4493509	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Information Disclosure	4493509	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Information Disclosure	4493509	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Information Disclosure	4493509	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0889 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0889 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0889						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4499164 Monthly Rollup 4499175	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0889						
Itanium-Based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0889						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0889						
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4499149 Monthly Rollup	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7	Yes

CVE-2019-0889						
Systems Service Pack 2	4499180 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0890 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0890						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4499164 Monthly Rollup 4499175	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0890						
Itanium-Based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
	Only					
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
x64-based Systems						
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for	4497936 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0890						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0890						
Core installation)						

CVE-2019-0891 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0891 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Are Active Directory and Exchange Server affected by this vulnerability? No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0891						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0891						
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
(Server Core installation)	Only					
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
	Only					
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7	Yes

CVE-2019-0891						
Core installation)	4499165 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0891						
32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
based Systems						
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0891						
(Server Core installation)						

CVE-2019-0892 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0892 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how Win32k handles objects in memory.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0892						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0892						
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0892						
(Server Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0892						
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0892						
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0893 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0893 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0893						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0893						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0893						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0893						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0893						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0894 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0894						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0894						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0894						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0894						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0894						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0895 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0895						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0895						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0895						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0895						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0895						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0896 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0896						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0896						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0896						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0896						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0896						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0897 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0897						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0897						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0897						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0897						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0897						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0898 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0898						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0898						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0898						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0898						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0898						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0899 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0899						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0899						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0899						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0899						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0899						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0900 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0900						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0900						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0900						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0900						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0900						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0901 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0901						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0901						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0901						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0901						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0901						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0902 MITRE NVD	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** **Are Active Directory and Exchange Server affected by this vulnerability?** No, Active Directory and Exchange Server are not affected. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2019-0902						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4499164 Monthly Rollup 4499175 Security	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4499164 Monthly Rollup	Important	Remote Code Execution	4493472	Base: 7.8 Temporal: 7	Yes

CVE-2019-0902						
based Systems Service Pack 1	4499175 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4499158 Security Only	Important	Remote Code Execution	4493451	Base: 7.8 Temporal: 7	Yes

CVE-2019-0902						
Core installation)	4499171 Monthly Rollup				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
	Only					
Windows RT 8.1	4499151 Monthly Rollup	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Remote Code Execution	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Important	Remote Code Execution	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
Windows Server 2016	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
32-bit Systems						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4499179 Security	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7	Yes

CVE-2019-0902						
ARM64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
(Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4499149 Monthly Rollup 4499180 Security	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0902						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Remote Code Execution	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903 - GDI+ Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0903	**CVE Title:** GDI+ Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit the vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to open an email attachment or click a link in an email or instant message. • In a file-sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting the way that the Windows GDI handles objects in the memory.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0903						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0903						
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Critical	Remote Code Execution	4493472	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows Server 2012	4499158 Security Only 4499171 Monthly Rollup	Critical	Remote Code Execution	4493451	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Critical	Remote Code Execution	4493451	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Critical	Remote Code Execution	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Critical	Remote Code Execution	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Critical	Remote Code Execution	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security	Critical	Remote Code Execution	4493446	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
	Only					
Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows Server 2016 (Server Core installation)	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0903						
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4499149 Monthly Rollup	Critical	Remote Code Execution	4493471	Base: 8.8 Temporal: 7.9	Yes

CVE-2019-0903						
based Systems Service Pack 2	4499180 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Critical	Remote Code Execution	4493471	Base: 8.8 Temporal: 7.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0911 MITRE NVD	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0911						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11	4498206 IE Cumulativ	Critical	Remote Code	4493472	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0911						
on Windows 7 for 32-bit Systems Service Pack 1	e 4499164 Monthly Rollup		Execution		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	
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	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	4498206 IE Cumulative 4499164 Monthly Rollup	Moderate	Remote Code Execution	4493472	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
Systems Service Pack 1						
Internet Explorer 11 on Windows Server 2012	4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	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 32-bit systems	4498206 IE Cumulative 4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4498206 IE Cumulative 4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
Internet Explorer 11 on Windows Server 2012 R2	4498206 IE Cumulative 4499151 Monthly Rollup	Moderate	Remote Code Execution	4493446	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 RT 8.1	4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4499154 Security Update	Critical	Remote Code Execution	4493475	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-	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
based Systems						
Internet Explorer 11 on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	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 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	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	4499181 Security Update	Critical	Remote Code Execution	4493474	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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
1709 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	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	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2019-0911						
10 Version 1803 for x64-based Systems					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	
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	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	4494441 Security	Critical	Remote Code	4493509	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0911						
on Windows 10 Version 1809 for x64-based Systems	Update		Execution		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	
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	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	4499179 Security	Critical	Remote Code	4493441	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0911						
on Windows 10 Version 1709 for ARM64-based Systems	Update		Execution		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	
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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	4498206 IE Cumulative 4499171 Monthly Rollup	Moderate	Remote Code Execution	4493451	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
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security	Critical	Remote Code	4493475	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0911						
Windows 10 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security	Critical	Remote Code	4493441	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0911						
Windows 10 Version 1709 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
1803 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
ARM64-based Systems						
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0911						
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0912 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0912 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0912						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0912						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0912						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0912						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0912						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0912						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0912						
ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0913 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0913 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0913						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0913						
Microsoft Edge on Windows 10 for x64-based Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0913						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0913						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0913						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0913						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0913						
10 Version 1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0913						
	Update					

CVE-2019-0914 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0914 MITRE NVD	**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.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0914						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0914						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0914						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0914						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0914						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0914						
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0914						
1903 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0915 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0915 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0915						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0915						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0915						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0915						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0915						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0915						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0915						
ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0916 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0916 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0916						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0916						
Microsoft Edge on Windows 10 for x64-based Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0916						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0916						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0916						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0916						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0916						
10 Version 1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0916						
	Update					

CVE-2019-0917 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0917 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0917						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0917						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0917						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0917						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0917						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0917						
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0917						
1903 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0918 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0918 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0918						
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	4499149 Monthly Rollup 4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	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 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	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	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	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	4498206 IE Cumulative 4499164 Monthly	Moderate	Remote Code Execution	4493472	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
Server 2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows Server 2012	4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	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 32-bit systems	4498206 IE Cumulative 4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4498206 IE Cumulative 4499151	Critical	Remote Code Execution	4493446	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0918						
Windows 8.1 for x64-based systems	Monthly Rollup				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	
Internet Explorer 11 on Windows Server 2012 R2	4498206 IE Cumulative 4499151 Monthly Rollup	Moderate	Remote Code Execution	4493446	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 RT 8.1	4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
Internet Explorer 11 on Windows 10 for x64-based Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	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	4494440 Security Update	Moderate	Remote Code Execution	4493470	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 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	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	4499181 Security Update	Critical	Remote Code Execution	4493474	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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	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-	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	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	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
10 Version 1809 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0918						
10 Version 1903 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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	4498206 IE Cumulative 4499171 Monthly Rollup	Moderate	Remote Code Execution	4493451	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0921 - Internet Explorer Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0921 MITRE NVD	**CVE Title:** Internet Explorer Spoofing Vulnerability **Description:** An spoofing vulnerability exists when Internet Explorer improperly handles URLs. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by changing how URLs are handled by Internet Explorer. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0921						
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	4499149 Monthly Rollup 4498206 IE Cumulative	Low	Spoofing	4493435	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4498206 IE Cumulative	Low	Spoofing	4493435	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0921						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Important	Spoofing	4493472	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/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Important	Spoofing	4493472	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/RC:C	Yes
Internet Explorer 11 on Windows Server	4498206 IE Cumulative 4499164 Monthly	Low	Spoofing	4493472	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0921						
2008 R2 for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows Server 2012	4498206 IE Cumulative	Low	Spoofing	4493435	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4498206 IE Cumulative 4499151 Monthly Rollup	Important	Spoofing	4493446	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/RC:C	Yes
Internet Explorer 11 on Windows	4498206 IE Cumulative 4499151 Monthly	Important	Spoofing	4493446	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/RC:C	Yes

CVE-2019-0921						
8.1 for x64-based systems	Rollup					
Internet Explorer 11 on Windows Server 2012 R2	4498206 IE Cumulative 4499151 Monthly Rollup	Low	Spoofing	4493446	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4499151 Monthly Rollup	Important	Spoofing	4493446	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/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Spoofing	4493475	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/RC:C	Yes

CVE-2019-0921						
Internet Explorer 11 on Windows 10 for x64-based Systems	4499154 Security Update	Important	Spoofing	4493475	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/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4494440 Security Update	Low	Spoofing	4493470	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Spoofing	4493470	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/RC:C	Yes

CVE-2019-0921						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Spoofing	4493470	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Spoofing	4493474	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/RC:C	Yes
Internet Explorer 11 on Windows	4499181 Security Update	Important	Spoofing	4493474	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/RC:C	Yes

CVE-2019-0921						
10 Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Spoofing	4493441	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-	4499179 Security Update	Important	Spoofing	4493441	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/RC:C	Yes

CVE-2019-0921						
based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Spoofing	4493464	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Spoofing	4493464	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/RC:C	Yes
Internet Explorer	4499167 Security	Important	Spoofing	4493464	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0921						
11 on Windows 10 Version 1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Spoofing	4493509	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4494441 Security Update	Important	Spoofing	4493509	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/RC:C	Yes

CVE-2019-0921						
1809 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Spoofing	4493509	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/RC:C	Yes
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Low	Spoofing	4493509	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4499179 Security	Important	Spoofing	4493441	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0921						
Windows 10 Version 1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Spoofing	4493441	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/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for	4497936 Security Update	Important	Spoofing	4493441	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/RC:C	Yes

CVE-2019-0921						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Spoofing	4493441	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/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4498206 IE Cumulative 4499171 Monthly Rollup	Low	Spoofing	4493451	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0922 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0922						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0922						
ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0923 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0923 MITRE NVD	**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	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0923						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4494440 Security Update	Low	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10	4494440 Security	Important	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0923						
Version 1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-0923						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1803	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-0923						
for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-0923						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Low	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1903	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-0923						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2019-0924 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0924 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0924						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0924						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0924						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0924						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0924						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0924						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0924						
ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0925 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0925 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0925						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0925						
10 Version 1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0925						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0925						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0925						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0925						
1709 for ARM64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0925						
ARM64-based Systems						
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0926 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0926 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0926						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0926						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0926						
10 Version 1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0927 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0927 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0927						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0927						
10 Version 1703 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0927						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0927						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0927						
based Systems						
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0927						
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0929 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0929 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0929						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	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	4499167 Security	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0929						
Windows 10 Version 1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4494441 Security Update	Critical	Remote Code Execution	4493509	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-2019-0929						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	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	4497936 Security Update	Critical	Remote Code Execution	4493509	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-2019-0929						
Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493509	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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493509	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-2019-0930 - Internet Explorer Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0930 MITRE NVD	**CVE Title:** Internet Explorer Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Internet Explorer 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 security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What type of information could be disclosed by this vulnerability? The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0930						
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	4499149 Monthly Rollup 4498206 IE Cumulative	Low	Information Disclosure	4493435	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	4499149 Monthly Rollup 4498206 IE Cumulative	Low	Information Disclosure	4493435	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-2019-0930						
Service Pack 2						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Important	Information Disclosure	4493472	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	4498206 IE Cumulative 4499164 Monthly Rollup	Important	Information Disclosure	4493472	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Low	Information Disclosure	4493472	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 Server 2012	4498206 IE Cumulative	Low	Information Disclosure	4493435	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	4498206 IE Cumulative 4499151 Monthly	Important	Information Disclosure	4493446	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
32-bit systems	Rollup					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4498206 IE Cumulative 4499151 Monthly Rollup	Important	Information Disclosure	4493446	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	4498206 IE Cumulative 4499151 Monthly Rollup	Low	Information Disclosure	4493446	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	4499151 Monthly Rollup	Important	Information Disclosure	4493446	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Information Disclosure	4493475	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	4499154 Security Update	Important	Information Disclosure	4493475	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	4494440 Security Update	Low	Information Disclosure	4493470	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-2019-0930						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Information Disclosure	4493470	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	4494440 Security Update	Important	Information Disclosure	4493470	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 Window	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-0930						
s 10 Version 1703 for 32-bit Systems					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	
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Information Disclosure	4493474	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	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	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	4494441 Security	Important	Information Disclosure	4493509	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-0930						
Windows 10 Version 1809 for 32-bit Systems	Update				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	
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Low	Information Disclosure	4493509	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	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 Window	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2019-0930						
s 10 Version 1903 for 32-bit Systems					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	
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	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 1903 for ARM64-	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0930						
based Systems						
Internet Explorer 10 on Windows Server 2012	4498206 IE Cumulative 4499171 Monthly Rollup	Low	Information Disclosure	4493451	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-2019-0931 - Windows Storage Service Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0931 MITRE NVD	**CVE Title:** Windows Storage Service Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations. An attacker who successfully exploited this vulnerability could gain elevated privileges on the victim system. To exploit the vulnerability, an attacker would first have to gain execution on the victim system, then run a specially crafted application. The security update addresses the vulnerability by correcting how the Storage Services handles file operations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0931						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	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	4499181 Security Update	Important	Elevation of Privilege	4493474	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	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0931						
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0931						
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0931						
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	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 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	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 1903 for	4497936 Security	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3	Yes

CVE-2019-0931						
x64-based Systems	Update				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	
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	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 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0932 - Skype for Android Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0932 MITRE NVD	**CVE Title:** Skype for Android Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Skype for Android. An attacker that exploited the vulnerability could listen to the conversation of a Skype for Android user without the userâ€™s knowledge. To exploit the vulnerability, an attacker would need to call an Android phone with Skype for Android installed thatâ€™s also paired with a Bluetooth device. The security update addresses the vulnerability by correcting how Skype for Android answers incoming calls. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is audio from a cellular phone call.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	How do I get the update for Skype for Android? 1. Tap the **Google Play** icon on your home screen. 2. Swipe in from the left edge of the screen. 3. Tap **My apps & games**. 4. Tap the Update box next to the **Skype app**. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0932						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Skype 8.35 when installed on Android Devices		Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	

CVE-2019-0933 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0933	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0933						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0933						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0933						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0933						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0933						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0933						
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0933						
1903 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0936 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0936 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows when Windows fails to properly handle certain symbolic links. An attacker who successfully exploited this vulnerability could potentially set certain items to run at a higher level and thereby elevate permissions. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows handles symbolic links. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0936						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based	4499164 Monthly Rollup 4499175 Security	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Elevation of Privilege	4493472	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4499158 Security Only 4499171 Monthly	Important	Elevation of Privilege	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
	Rollup					
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Elevation of Privilege	4493451	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows Server 2012 R2	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4499151 Monthly Rollup	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Elevation of Privilege	4493446	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
based Systems						
Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0936						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4499149 Monthly Rollup 4499180 Security Only	Important	Elevation of Privilege	4493471	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0937 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0937	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0937						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0937						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0937						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0937						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0937						
10 Version 1903 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0937						
	Update					

CVE-2019-0938 - Microsoft Edge Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0938 MITRE NVD	**CVE Title:** Microsoft Edge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser. An attacker who successfully exploited this vulnerability could gain elevated privileges and break out of the Edge AppContainer sandbox. The vulnerability by itself does not allow arbitrary code to run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (for example a remote code execution vulnerability and another elevation of privilege vulnerability) to take advantage of the elevated privileges when running. The security update addresses the vulnerability by modifying how Microsoft Edge handles sandboxing.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0938						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0938						
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Low	Elevation of Privilege	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0938						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0938						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0938						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0938						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Low	Elevation of Privilege	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security	Important	Elevation of Privilege	4493441	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0938						
10 Version 1709 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4497936 Security Update	Important	Elevation of Privilege	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0938						
1903 for ARM64-based Systems						

CVE-2019-0940 - Microsoft Browser Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0940 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0940						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	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	4498206 IE Cumulative 4499164 Monthly Rollup	Critical	Remote Code Execution	4493472	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Systems Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498206 IE Cumulative 4499164 Monthly Rollup	Moderate	Remote Code Execution	4493472	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	4498206 IE Cumulative	Moderate	Remote Code Execution	4493435	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	4498206 IE Cumulative 4499151	Critical	Remote Code Execution	4493446	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0940						
Windows 8.1 for 32-bit systems	Monthly Rollup				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	
Internet Explorer 11 on Windows 8.1 for x64-based systems	4498206 IE Cumulative 4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	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	4498206 IE Cumulative 4499151 Monthly Rollup	Moderate	Remote Code Execution	4493446	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 RT 8.1	4499151 Monthly Rollup	Critical	Remote Code Execution	4493446	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	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	4499154 Security Update	Critical	Remote Code Execution	4493475	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	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Critical	Remote Code Execution	4493470	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	4494440 Security Update	Critical	Remote Code Execution	4493470	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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
10 Version 1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	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	4494441 Security	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0940						
Windows 10 Version 1809 for 32-bit Systems	Update				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	
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	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	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
10 Version 1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	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 1903 for ARM64-	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
based Systems						
Internet Explorer 10 on Windows Server 2012	4498206 IE Cumulative 4499171 Monthly Rollup	Moderate	Remote Code Execution	4493451	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
Microsoft Edge on Windows 10 for 32-bit Systems	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499154 Security Update	Critical	Remote Code Execution	4493475	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Microsoft Edge on Windows Server 2016	4494440 Security Update	Moderate	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4494440 Security Update	Critical	Remote Code Execution	4493470	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499181 Security Update	Critical	Remote Code Execution	4493474	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Version 1803 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Critical	Remote Code Execution	4493464	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Critical	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4494441 Security Update	Moderate	Remote Code Execution	4493509	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/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 1903 for	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0940						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Critical	Remote Code Execution	4493441	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0942 - Unified Write Filter Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0942	**CVE Title:** Unified Write Filter Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists in the Unified Write Filter (UWF) feature for Windows 10 when it improperly restricts access to the registry. An attacker who successfully exploited the vulnerability could make changes to the registry keys protected by UWF without having administrator privileges. To exploit the vulnerability, an attacker would have to log on to an affected system utilizing UWF and access the registry editor. The security update addresses the vulnerability by correcting how the Unified Write Filter verifies privileges when accessing the registry. **FAQ:** **What is the Unified Write Filter feature?** Unified Write Filter (UWF) is an optional Windows 10 feature that helps to protect your drives by intercepting and redirecting any writes to the drive (app installations, settings changes, saved data) to a virtual overlay. The virtual overlay is a temporary location that is usually cleared during a reboot or when a guest user logs off. More information is available at https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/unified-write-filter		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0942						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4499154 Security	Important	Elevation of Privilege	4493475	Base: 4.4 Temporal: 4	Yes

CVE-2019-0942						
	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4499154 Security Update	Important	Elevation of Privilege	4493475	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Elevation of Privilege	4493470	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0942						
Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Elevation of Privilege	4493474	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0942						
Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Elevation of Privilege	4493464	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for	4494441 Security	Important	Elevation of Privilege	4493509	Base: 4.4 Temporal: 4	Yes

CVE-2019-0942						
x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Elevation of Privilege	4493509	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Elevation of Privilege	4493441	Base: 4.4 Temporal: 4 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2019-0945 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0945 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0945						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0945						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4464567 Security Update	Important	Remote Code Execution	4464520	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4464567 Security Update	Important	Remote Code Execution	4464520	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4464561 Security Update	Important	Remote Code Execution	4462204	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4464561 Security Update	Important	Remote Code Execution	4462204	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4464561 Security Update	Important	Remote Code Execution	4462204	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4464551 Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal:	Maybe

CVE-2019-0945						
					N/A Vector: N/A	
Microsoft Office 2016 (64-bit edition)	4464551 Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0946 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0946 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0946						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0946						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4464567 Security Update	Important	Remote Code Execution	4464520	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4464567 Security Update	Important	Remote Code Execution	4464520	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4464561 Security Update	Important	Remote Code Execution	4462204	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4464561 Security Update	Important	Remote Code Execution	4462204	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4464561 Security Update	Important	Remote Code Execution	4462204	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4464551 Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal:	Maybe

CVE-2019-0946						
					N/A Vector: N/A	
Microsoft Office 2016 (64-bit edition)	4464551 Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Important	Remote Code Execution	4462213	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0947 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0947 MITRE NVD	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0947						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0947						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4464567 Security Update	Important	Remote Code Execution	4464520	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4464567 Security Update	Important	Remote Code Execution	4464520	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0949 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0949 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing 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.	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0949						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Spoofing	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464549 Security Update	Important	Spoofing	4464510	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0950 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0950 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing 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:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Is the Preview Pane an attack vector for this vulnerability? No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0950						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Spoofing	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464549 Security Update	Important	Spoofing	4464510	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0951 - Microsoft SharePoint Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0951 MITRE NVD	**CVE Title:** Microsoft SharePoint Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0951						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2010 Service Pack 2	4464573 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0951						
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Spoofing	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0952 - Microsoft SharePoint Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0952 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls. An authenticated attacker who successfully exploited the vulnerability could use a specially crafted page to perform actions in the security context of the SharePoint application pool process. To exploit the vulnerability, an authenticated user must create and invoke a specially crafted page on an affected version of Microsoft SharePoint Server.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft SharePoint Server handles processing of created content. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0952						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Remote Code Execution	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464549 Security Update	Important	Remote Code Execution	4464510	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0953 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0953 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. To exploit the vulnerability, a user must open a specially crafted file with an affected version of Microsoft Word software. 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) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Word handles files in memory. **FAQ:** **Is the Preview Pane an attack vector for this vulnerability?** Yes, the Preview Pane is an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0953						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2016 for Mac	Release Notes Security Update	Critical	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4464536 Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4464536 Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2019 for 32-bit editions	Click to Run Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2019-0953						
Microsoft Office 2019 for 64-bit editions	Click to Run Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2019 for Mac	Release Notes Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 32-bit Systems	Click to Run Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	No
Office 365 ProPlus for 64-bit Systems	Click to Run Security Update	Critical	Remote Code Execution	4461543	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Online Server	4462169 Security Update	Critical	Remote Code Execution	4461633	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0956 - Microsoft SharePoint Server Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0956 MITRE NVD	**CVE Title:** Microsoft SharePoint Server Information Disclosure Vulnerability **Description:** An information disclosure 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Personally Identifiable Information (PII). **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0956						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Information Disclosure	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4464549 Security Update	Important	Information Disclosure	4464510	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0957 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0957 MITRE NVD	**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.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0957						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4464549 Security Update	Important	Elevation of Privilege	4464510	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2019	4464556 Security Update	Important	Elevation of Privilege	4464518	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0958 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0958	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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:** **Is the Preview Pane an attack vector for this vulnerability?** No, the Preview Pane is not an attack vector. **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0958						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Elevation of Privilege	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0958						
Microsoft SharePoint Server 2019	4464556 Security Update	Important	Elevation of Privilege	4464518	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0961 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0961 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0961						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 4499175	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499164 Monthly Rollup 4499175 Security Only	Important	Information Disclosure	4493472	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499158 Security Only	Important	Information Disclosure	4493451	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0961						
	4499171 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4499158 Security Only 4499171 Monthly Rollup	Important	Information Disclosure	4493451	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows 8.1 for x64-based systems	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499151 Monthly Rollup	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows Server 2012 R2 (Server Core installation)	4499151 Monthly Rollup 4499165 Security Only	Important	Information Disclosure	4493446	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499154 Security Update	Important	Information Disclosure	4493475	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499154 Security Update	Important	Information Disclosure	4493475	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0961						
	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4494440 Security Update	Important	Information Disclosure	4493470	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Information Disclosure	4493474	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for	4499167 Security	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2019-0961						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Information Disclosure	4493464	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4494441 Security Update	Important	Information Disclosure	4493509	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for 32-bit Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for x64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1903 for ARM64-based Systems	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
Windows Server, version 1903 (Server Core installation)	4497936 Security Update	Important	Information Disclosure	4493441	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4499149 Monthly Rollup 4499180 Security	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0961						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4499149 Monthly Rollup 4499180 Security Only	Important	Information Disclosure	4493471	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0963 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0963 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Is the Preview Pane an attack vector for this vulnerability? No, the Preview Pane is not an attack vector. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0963						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4464564 Security Update	Important	Spoofing	4464515	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0971 - Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0971 MITRE NVD	**CVE Title:** Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Azure DevOps Server and Microsoft Team Foundation Server do not properly sanitize a specially crafted authentication	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	request to an affected server. An attacker who successfully exploited this vulnerability could execute malicious code on a vulnerable server. To exploit this vulnerability, an authenticated attacker would need to create a page specifically designed to cause a server-side request. The attacker would then send a specially-crafted message to perform a server-side request forgery attack. The update addresses the vulnerability by modifying how Azure DevOps Server and Microsoft Team Foundation Server manage server authentication. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is device information like resource ids, sas tokens, user properties, and other sensitive information. **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0971						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe
Azure DevOps Server 2019	Release Notes Security Update	Important	Information Disclosure		Base: N/A Temporal:	Maybe

CVE-2019-0971						
					N/A Vector: N/A	

CVE-2019-0976 - NuGet Package Manager Tampering Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0976 MITRE NVD	**CVE Title:** NuGet Package Manager Tampering Vulnerability **Description:** A tampering vulnerability exists in the NuGet Package Manager for Linux and Mac that could allow an authenticated attacker to modify contents of the intermediate build folder (by default â€œobjâ€□). An attacker who successfully exploited this vulnerability could potentially modify files and folders that impact binaries created as part of building a project. To exploit this vulnerability, an attacker would need to log on to the affected system and tamper with the intermediate build folder which may impact the output of future builds of that project. The security update addresses the vulnerability by correcting permissions on the intermediate build folder.	Important	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0976						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0976						
Nuget 5.0.2	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0979 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0979 MITRE NVD	**CVE Title:** Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability **Description:** A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to an Azure DevOps server or a Team Foundation server, which will get executed in the context of the user every time a user visits the compromised page. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. The security update addresses the vulnerability by ensuring that Azure DevOps Server and Team Foundation Server properly sanitize user inputs. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0979						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2017 Update 3.1	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2018 Update 1.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Azure DevOps Server 2019	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980 - .Net Framework and .Net Core Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0980 MITRE NVD	**CVE Title:** .Net Framework and .Net Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Framework or .NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Framework or .NET Core application. The update addresses the vulnerability by correcting how .NET Framework or .NET Core web applications handles web requests. **FAQ:** None **Mitigations:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0980						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961	Important	Denial of Service		Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4498962 Security Only 4499407	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4498963 Security Only	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal:	Maybe

CVE-2019-0980						
	4499408 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal:	Maybe

CVE-2019-0980						
	4499409 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2 on Windows 10 for x64-based Systems	4499154 Security	Important	Denial of Service	4493475	Base: N/A Temporal:	Yes

CVE-2019-0980						
	Update				N/A Vector: N/A	
.NET Core 1.0	Release Notes Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 1.1	Release Notes Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0980						
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems	4499167 Security	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Yes

CVE-2019-0980						
	Update				Vector: N/A	
Microsoft .NET Framework 4.7.2 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
	Security Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4499408 Monthly	Important	Denial of Service	4495165	Base: N/A Temporal:	Maybe

CVE-2019-0980						
	Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A	Yes

CVE-2019-0980						
					Vector: N/A	
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0980						
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.1	Release Notes Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 2.2	Release Notes Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012	4498962 Security Only	Important	Denial of Service	4493441	Base: N/A Temporal:	Maybe

CVE-2019-0980						
	4499407 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4495611 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4495611 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Update				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4495613 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4495613 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2019 (Server Core installation)	4499405 Monthly	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1903 (Server Core installation)	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
	Rollup					
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0980						
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4499181 Security	Important	Denial of Service	4493474	Base: N/A Temporal: N/A	Yes

CVE-2019-0980						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0980						
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019	4499405 Monthly	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
Microsoft .NET Framework 3.5 on Windows Server, version 1903 (Server Core installation)	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406 Monthly	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0980						
	Rollup					
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A	Maybe

CVE-2019-0980						
	Monthly Rollup				Vector: N/A	

CVE-2019-0981 - .Net Framework and .Net Core Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0981 MITRE NVD	**CVE Title:** .Net Framework and .Net Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Framework or .NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Framework or .NET Core application.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how .NET Framework or .NET Core web applications handles web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0981						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4498963 Security Only	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal:	Maybe

CVE-2019-0981						
	4499408 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal:	Maybe

CVE-2019-0981						
	4499409 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 4.6.2 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2 on Windows 10 for x64-based Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 1.0	Release Notes Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 1.1	Release Notes Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Yes

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.2 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1	4499406 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	4498961 Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4499406 Monthly Rollup 4498961 Security Only	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012	4498962 Security Only	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal:	Maybe

CVE-2019-0981						
	4499407 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0981						
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems	4499181 Security	Important	Denial of Service	4493474	Base: N/A Temporal: N/A	Yes

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.1	Release Notes Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
.NET Core 2.2	Release Notes Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
	Rollup					
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows RT 8.1	4499408 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Rollup				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows Server 2016	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)	4495610 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems	4495611 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems	4495611 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems	4495613 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems	4495613 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems	4495616 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)	4495616 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 4.8 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.8 on Windows Server, version 1903 (Server Core installation)	4495620 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4498962 Security Only 4499407 Monthly Rollup	Important	Denial of Service	4487079; 4487257	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4498963 Security Only 4499408	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4498963 Security Only 4499408 Monthly Rollup	Important	Denial of Service	4489488; 4495165	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4499154 Security Update	Important	Denial of Service	4493475	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4499154 Security	Important	Denial of Service	4493475	Base: N/A Temporal: N/A	Yes

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2016	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4494440 Security Update	Important	Denial of Service	4493470	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0981						
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Denial of Service	4493474	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security	Important	Denial of Service	4493464	Base: N/A Temporal: N/A	Yes

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems	4499167 Security Update	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)	4499405 Monthly Rollup	Important	Denial of Service	4493464	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for 32-bit Systems	4495620 Security	Important	Denial of Service	4493441	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for x64-based Systems	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server, version 1903 (Server Core installation)	4495620 Security Update	Important	Denial of Service	4493441	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0981						
	Rollup					
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4498964 Security Only 4499409 Monthly Rollup	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4498964 Security Only 4499409	Important	Denial of Service	4487081; 4487259	Base: N/A Temporal: N/A	Maybe

CVE-2019-0981						
	Monthly Rollup				Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4498961 Security Only	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal:	Maybe

CVE-2019-0981						
	4499406 Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4498961 Security Only 4499406 Monthly Rollup	Important	Denial of Service	4487078; 4487256	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0982 - ASP.NET Core Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0982 MITRE NVD	**CVE Title:** ASP.NET Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the ASP.NET Core application. The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests. **FAQ:** **How do I know if my client or server app is vulnerable?** A client or server app is vulnerable if it has a package reference to these versions of Microsoft.AspNetCore.SignalR.Protocols.MessagePack: • For 2.2.x apps: MessagePack 1.1.0 is vulnerable, and the fix is in 1.1.5 • For 2.1.x apps: MessagePack 1.0.4 (and earlier), and the fix is in 1.0.11 **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0982						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.1	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 2.2	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0995 - Internet Explorer Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0995 MITRE NVD	**CVE Title:** Internet Explorer Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when urlmon.dll improperly handles certain Mark of the Web queries. The vulnerability allows Internet Explorer to bypass Mark of the Web warnings or restrictions for files downloaded or created in a specific way. In a web-based attack scenario, an attacker would need to host a malicious file that is designed to exploit the vulnerability and then convince a user to download the malicious file and then open the file in Internet Explorer. The security update addresses the vulnerability by modifying how urlmon.dll handles Mark of the Web queries. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0995						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows Server 2016	4494440 Security Update	Low	Security Feature Bypass	4493470	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0995						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4494440 Security Update	Important	Security Feature Bypass	4493470	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4494440 Security Update	Important	Security Feature Bypass	4493470	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4499181 Security Update	Important	Security Feature Bypass	4493474	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0995						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4499181 Security Update	Important	Security Feature Bypass	4493474	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4499179 Security Update	Important	Security Feature Bypass	4493441	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4499179 Security Update	Important	Security Feature Bypass	4493441	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0995						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-	4499167 Security Update	Important	Security Feature Bypass	4493464	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0995						
based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1809 for	4494441 Security Update	Important	Security Feature Bypass	4493509	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0995						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4494441 Security Update	Low	Security Feature Bypass	4493509	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4499179 Security Update	Important	Security Feature Bypass	4493441	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4497936 Security Update	Important	Security Feature Bypass	4493441	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0995						
1903 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems	4497936 Security Update	Important	Security Feature Bypass	4493441	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems	4497936 Security Update	Important	Security Feature Bypass	4493441	Base: 7.3 Temporal: 6.6 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-1000 - Microsoft Azure AD Connect Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1000 MITRE NVD	**CVE Title:** Microsoft Azure AD Connect Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Azure Active Directory Connect build 1.3.20.0, which allows an attacker to execute two PowerShell cmdlets in context of a privileged account, and perform privileged actions. To exploit this, an attacker would need to authenticate to the AzureÂ AD Connect server. These cmdlets can be executed remotely only if remote access is enabled on the Azure AD Connect server. This security update address the issue by disabling these cmdlets. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1000						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Azure Active Directory Connect	Release Notes Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-1008 - Microsoft Dynamics On-Premise Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-1008 MITRE NVD	**CVE Title:** Microsoft Dynamics On-Premise Security Feature Bypass **Description:** A security feature bypass vulnerability exists in Dynamics On Premise. An attacker who exploited the vulnerability could send attachment types that are blocked by the email attachment system. To exploit the vulnerability, an attacker would need to capture and edit the POST request to include a special character in the extension. The update addresses the vulnerability by blocking files with the special character in the file extension. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 05/14/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-1008						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Dynamics 365 (on-premises) version 8.2	4494412 Security Update	Important	Security Feature Bypass		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Dynamics 365 (on-premises) version 9.0	4498363 Security Update	Important	Security Feature Bypass		Base: N/A Temporal:	Maybe

CVE-2019-1008						
					N/A Vector: N/A	
Microsoft Dynamics CRM 2015 (on-premises) version 7.0	4499386 Security Update	Important	Security Feature Bypass		Base: N/A Temporal: N/A Vector: N/A	Maybe

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