微软发布 1 月补丁修复 59 个安全问题

安全威胁通告

发布时间：2018 年 1 月 10 日

综述

微软于周二发布了 1 月安全更新补丁，修复了 59 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 Framework、Adobe Flash Player、ASP .NET、ASP.NET、Graphic Fonts、Microsoft Browsers、Microsoft Edge、Microsoft Graphics Component、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows、Side-Channel、Windows Kernel、Windows SMB Server 以及 Windows Subsystem for Linux。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE 编号	CVE 标题
.NET Framework	CVE-2018-0786	.NET 安全功能绕过漏洞
.NET Framework	CVE-2018-0764	.NET and .NET Core 拒绝服务漏洞
Adobe Flash Player	ADV180001	January 2018 Adobe Flash 安全更新
ASP .NET	CVE-2018-0784	ASP.NET Core 特权提升漏洞
ASP.NET	CVE-2018-0785	ASP.NET Core CSRF 漏洞
Graphic Fonts	CVE-2018-0788	OpenType Font Driver 特权提升漏洞
Graphic Fonts	CVE-2018-0754	OpenType Font Driver 信息泄露漏洞

Microsoft Browsers	CVE-2018-0762	Scripting Engine 内存破坏漏洞
Microsoft Browsers	CVE-2018-0772	Scripting Engine 内存破坏漏洞
Microsoft Edge	CVE-2018-0803	Microsoft Edge 特权提升漏洞
Microsoft Edge	CVE-2018-0766	Microsoft Edge 信息泄露漏洞
Microsoft Graphics Component	CVE-2018-0750	Windows GDI 信息泄露漏洞
Microsoft Graphics Component	CVE-2018-0741	Microsoft Color Management 信息泄露漏洞
Microsoft Office	ADV180003	Microsoft Office Defense in Depth Update
Microsoft Office	CVE-2018-0804	Microsoft Word 远程代码执行漏洞

Microsoft Office	CVE-2018-0805	Microsoft Word 远程代码执行漏洞
Microsoft Office	CVE-2018-0806	Microsoft Word 远程代码执行漏洞
Microsoft Office	CVE-2018-0807	Microsoft Word 远程代码执行漏洞
Microsoft Office	CVE-2018-0812	Microsoft Word 内存破坏漏洞
Microsoft Office	CVE-2018-0819	欺骗漏洞 in Microsoft Office for MAC
Microsoft Office	CVE-2018-0795	Microsoft Office 远程代码执行漏洞
Microsoft Office	CVE-2018-0797	Microsoft Word 内存破坏漏洞
Microsoft Office	CVE-2018-0799	Microsoft Access Tampering Vulnerability

Microsoft Office	CVE-2018-0802	Microsoft Office 内存破坏漏洞
Microsoft Office	CVE-2018-0801	Microsoft Office 远程代码执行漏洞
Microsoft Office	CVE-2018-0789	Microsoft SharePoint 特权提升漏洞
Microsoft Office	CVE-2018-0790	Microsoft SharePoint Cross Site Scripting 特权提升漏洞
Microsoft Office	CVE-2018-0791	Microsoft Outlook 远程代码执行漏洞
Microsoft Office	CVE-2018-0792	Microsoft Word 远程代码执行漏洞
Microsoft Office	CVE-2018-0793	Microsoft Outlook 远程代码执行漏洞
Microsoft Office	CVE-2018-0794	Microsoft Word 远程代码执行漏洞

Microsoft Office	CVE-2018-0796	Microsoft Excel 远程代码执行漏洞
Microsoft Office	CVE-2018-0798	Microsoft Office 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0818	Scripting Engine 安全特征绕过
Microsoft Scripting Engine	CVE-2018-0773	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0774	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0781	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0800	Scripting Engine 信息泄露漏洞
Microsoft Scripting Engine	CVE-2018-0758	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2018-0767	Scripting Engine 信息泄露漏洞
Microsoft Scripting Engine	CVE-2018-0768	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0769	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0770	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0775	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0776	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0777	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2018-0778	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2018-0780	Scripting Engine 信息泄露漏洞
Microsoft Windows	CVE-2018-0753	Windows IPSec 拒绝服务漏洞
Side-Channel	ADV180002	Guidance to mitigate speculative execution side-channel vulnerabilities
Windows Kernel	CVE-2018-0746	Windows 信息泄露漏洞
Windows Kernel	CVE-2018-0747	Windows 信息泄露漏洞
Windows Kernel	CVE-2018-0748	Windows 特权提升漏洞
Windows Kernel	CVE-2018-0751	Windows 特权提升漏洞
Windows Kernel	CVE-2018-0752	Windows 特权提升漏洞

Windows Kernel	CVE-2018-0744	Windows 特权提升漏洞
Windows Kernel	CVE-2018-0745	Windows 信息泄露漏洞
Windows SMB Server	CVE-2018-0749	SMB Server 特权提升漏洞
Windows Subsystem for Linux	CVE-2018-0743	Windows Subsystem for Linux 特权提升漏洞

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

附件

ADV180001 - January 2018 Adobe Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV180001 MITRE NVD	**CVE Title:** January 2018 Adobe Flash Security Update **Description:** This security update addresses the following vulnerability, which is described in Adobe Security Bulletin APSB18-01: CVE-2018-4871. **FAQ:** **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

ADV180001						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows Server 2012	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180001						
Adobe Flash Player on Windows 8.1 for 32-bit systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for 32-bit Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal:	Yes

ADV180001						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180001						
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems	4056887 Security Update	Critical	Remote Code Execution	4053577	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180002 - Guidance to mitigate speculative execution side-channel vulnerabilities

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV180002 MITRE NVD	**CVE Title:** Guidance to mitigate speculative execution side-channel vulnerabilities **Description:** Executive Summary Microsoft is aware of a new publicly disclosed class of vulnerabilities referred to as â€œspeculative execution side-channel attacksâ€ that affect many modern processors and operating systems including Intel, AMD, and ARM. Note: this issue will affect other systems such as Android, Chrome, iOS, MacOS, so we advise customers to seek out guidance from those vendors. Microsoft has released several updates to help mitigate these vulnerabilities. We have also taken action to secure our cloud services. See below for more details.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Microsoft has not received any 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. To get all available protections, hardware/firmware and software updates are required. This may include microcode from device OEMs and in some cases updates to AV software as well. This advisory addresses the following vulnerabilities: • CVE-2017-5753 - Bounds check bypass • CVE-2017-5715 - Branch target injection • CVE-2017-5754 - Rogue data cache load ## Recommended Actions For consumers, the best protection is to keep your computers up to date. You can do this by taking advantage of automatic update. Learn how to turn on automatic updates here. In addition to installing the January 2018 Windows security updates, you may also need to install firmware updates from your device manufacturer for increased protection. Check with your device manufacturer for relevant updates.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	If automatic updates are enabled, the January 2018 Windows security update will be offered to the devices running supported anti-virus (AV) applications. Updates can be installed in any order. 1. If you have automatic updating enabled and configured to provide updates for Windows, the updates are delivered to you when they are released, if your device and software are compatible. We recommend you verify these updates are installed. If automatic update is not enabled, manually check for and install the January 2018 Windows operating system security update. 2. Install applicable firmware update provided by your OEM device manufacturer. Customers using Surface products need to apply both firmware and software updates. See Microsoft Knowledge Base Article 4073065Â article for more information.Â Â # Potential performance impacts In testing Microsoft has seen some performance impact with these mitigations. For most consumer devices, the impact may not be noticeable, however, the specific impact varies by hardware generation and implementation by the chip manufacturer.â€¯Microsoft values the security of its software and services and has		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	made the decision to implement certain mitigation strategies in an effort to better secure our products. We continue to work with hardware vendors to improve performance while maintaining a high level of security. Advisory Details Vulnerabilities Description Speculative execution side-channel vulnerabilities can be used to read the content of memory across a trusted boundary and can therefore lead to information disclosure. There are multiple vectors by which an attacker could trigger the vulnerabilities depending on the configured environment. Microsoft has been working with hardware and software makers to jointly develop mitigations to protect customers across Microsoftâ€™s products and services. These mitigations prevent attackers from triggering a weakness in the CPU which could allow the contents of memory to be disclosed.		

Microsoft Windows client customers

In client scenarios, a malicious user mode application could be used to disclose the contents of kernel memory.

Customers using Windows client operating systems including Windows 7 Service Pack 1, Windows 8.1, and Windows 10 need to apply both firmware and software updates. See Microsoft Knowledge Base Article 4073119 for additional information.

Customers using Microsoft Surface and Surface Book products need to apply both firmware and software updates. Most customers have automatic updating enabled and will not need to take any action because this security update will be downloaded and installed automatically.

Microsoft will continue to work closely with industry partners to improve mitigations against this class of vulnerabilities.

Microsoft Windows Server customers

In server scenarios, a malicious user-mode application could be used to disclose the contents of kernel memory. In other multi-tenant hosting environments, a virtual

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	machine could read the memory of the host operating system or the memory of other guest operating systems running on the same physical machine. Customers using Windows server operating systems including Windows Server 2008 R2 Service Pack 1, Windows Server 2012 R2, and Windows Server 2016 need to apply firmware and software updates as well as configure protections. See Microsoft Knowledge Base Article 4072698 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 found here. Microsoft will continue to work closely with industry partners to improve mitigations against this class of vulnerabilities. ## Microsoft cloud customers Microsoft has already deployed mitigations across the majority of our cloud services and is accelerating efforts to complete the remainder.Â More information is available here.		

Microsoft SQL Server customers

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

FAQ

1. What systems are at risk from this vulnerability?

- **Client Operating Systems Windows** Windows client systems are at risk
- **Server Operating Systems** Windows servers are at risk

2. What are the associated CVEs for these vulnerabilities?

- See CVE-2017-5715
- See CVE-2017-5753
- See CVE-2017-5754

3. Have there been any active attacks detected?

No. When this security advisory was issued, Microsoft had not received any information to indicate that these vulnerabilities had been used to attack customers.

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	4. Have these vulnerabilities been publicly disclosed? Yes. The vulnerabilities were disclosed on January 3, 2018 at https://bugs.chromium.org/p/project-zero/issues/detail?id=1272 **5. I was not offered the Windows security updates released on January 3, 2018. What should I do?** To help avoid adversely affecting customer devices, the Windows security updates released on January 3rd, 2018 have only been offered to devices running compatible antivirus software. Please see Microsoft Knowledge Base Article 4072699 for more information about how to get the updates. **6. Why aren't Windows Server 2008 and Windows Server 2012 platforms getting an update? When can customers expect the fix?** Addressing a hardware vulnerability with a software update presents significant challenges with some operating systems requiring extensive architectural changes. Microsoft continues to work with affected chip manufacturers and investigate the best way to provide mitigations **7. I have an x86 architecture and the PowerShell Verification output indicates that I am not fully protected from these speculative execution side-channel vulnerabilities. Will Microsoft provide complete protections in the future?**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Addressing a hardware vulnerability with a software update presents significant challenges and mitigations for older operating systems that require extensive architectural changes. The existing 32 bit update packages listed in this advisory fully address CVE-2017-5753 and CVE-2017-5715, but do not provide protections for CVE-2017-5754 at this time. Microsoft is continuing to work with affected chip manufacturers and investigate the best way to provide mitigations for x86 customers, which may be provided in a future update. ## Additional suggested actions • **Protect your PC** We continue to encourage customers to follow our Protect Your Computer guidance of enabling a firewall, getting software updates, and installing antivirus software. For more information, see Microsoft Safety & Security Center. • **Keep Microsoft software updated** Users running Microsoft software should apply the latest Microsoft security updates to help make sure that their computers are as protected as possible. If you are not sure whether your software is up to date, visit Microsoft Update, scan your computer for available updates, and install any high-priority updates that are offered to you. If you have automatic updating enabled and configured to provide updates for		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Microsoft products, the updates are delivered to you when they are released, but you should verify that they are installed. ## Acknowledgments - Jann Horn of Google Project Zero - Paul Kocher - Moritz Lipp from Graz University of Technology - Daniel Genkin from University of Pennsylvania and University of Maryland - Daniel Gruss from Graz University of Technology - Werner Haas of Cyberus Technology GmbH - Mike Hamburg of Rambus Security Division - Stefan Mangard from Graz University of Technology - Thomas Prescher of Cyberus Technology GmbH - Michael Schwarz from Graz University of Technology - Yuval Yarom of The University of Adelaide and Data61 - Additional information on the Meltdown and Spectre attacks can be found at their respective web sites. - Anders Fogh of GDATA Advanced Analytics		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 4.0 01/09/2018 08:00:00 Revised the Affected Products table to include updates for supported editions of Microsoft SQL Server 2008, Microsoft SQL Server 2008, and Microsoft SQL Server 2016 because these updates provide mitigations for ADV180002. 1.0 01/03/2018 08:00:00 Information published. 2.0 01/03/2018 08:00:00 Revised ADV180002 to announce release of SQL 2016 and 2017 updates. 3.0 01/05/2018 08:00:00 The following updates have been made: Revised the Affected Products table to include Windows 10 Version 1709 for x64-based Systems because the update provides mitigations for ADV180002. Corrected the security update numbers for the 2016 and		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2017 SQL Server Cumulative Updates. Removed Windows Server 2012 and Windows Server 2012 (Server Core installation) from the Affected Products table because there are no mitigations available for ADV180002 for these products. Revised the Affected Products table to include Monthly Rollup updates for Windows 7 and Windows Server 2008 R2. Customers who install monthly rollups should install these updates to receive the mitigations against the vulnerabilities discussed in this advisory. In the Recommended Actions section, added information for Surface customers. Added an FAQ to explain why Windows Server 2008 and Windows Server 2012 will not receive mitigations for these vulnerabilities. Added an FAQ to explain the protection against these vulnerabilties for customers using x86 architecture.		

Affected Software

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

ADV180002						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

ADV180002						
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897	Important	Information Disclosure	4054518	Base: N/A Temporal:	Yes

ADV180002						
	Security Only				N/A Vector: N/A	
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	4056898 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	4056898 Security Only	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056568 IE Cumulative	Important	Information Disclosure	4052978	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056568 IE	Important	Information Disclosure	4052978	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180002						
	Cumulative					
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056568 IE Cumulative	Important	Information Disclosure	4052978	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4056895 Monthly Rollup 4056568 IE Cumulative	Important	Information Disclosure	4052978	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4056895 Monthly Rollup 4056568 IE Cumulative	Important	Information Disclosure	4052978	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2012 R2	4056895 Monthly Rollup 4056568 IE Cumulative	Important	Information Disclosure	4052978	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180002						
Internet Explorer 11 on Windows RT 8.1	4056895 Monthly Rollup	Important	Information Disclosure	4054519	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2016	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal:	Yes

ADV180002						
					N/A Vector: N/A	
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180002						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: N/A Temporal:	Yes

ADV180002						
					N/A Vector: N/A	
Microsoft Edge on Windows Server 2016	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180002						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: N/A Temporal:	Yes

ADV180002						
					N/A Vector: N/A	
Windows Server 2016	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SQL Server 2016 for x64-based Systems	4058560 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV180002						
Microsoft SQL Server 2016 for x64-based Systems (CU)	4058559 Security Update	Important	Information Disclosure	4053579	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1	4057118 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU)	4058561 Security Update	Important	Information Disclosure	4053580	Base: N/A Temporal: N/A Vector: N/A	Maybe
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal:	Yes

ADV180002						
					N/A Vector: N/A	
Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft SQL Server 2008 for 32-bit Systems Service Pack 4 (QFE)	4057114 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2017 for x64-based Systems	4057122 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2017 for x64-based Systems (CU)	4058562 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV180002						
Microsoft SQL Server 2008 R2 for 32-Bit Systems Service Pack 3 (QFE)	4057113 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2008 R2 for x64-Based Systems Service Pack 3 (QFE)	4057113 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2008 for x64-Based Systems Service Pack 4 (QFE)	4057114 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV180003 - Microsoft Office Defense in Depth Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV180003 MITRE NVD	**CVE Title:** Microsoft Office Defense in Depth Update **Description:** Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure.	None	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

ADV180003						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

ADV180003						
Microsoft Office 2007 Service Pack 3	4011201 Security Update	None	Defense in Depth	4011063	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011611 Security Update	None	Defense in Depth	4011055	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011611 Security Update	None	Defense in Depth	4011055	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011636 Security Update	None	Defense in Depth	4011103	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011636 Security Update	None	Defense in Depth	4011103	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4011636 Security Update	None	Defense in Depth	4011103	Base: N/A Temporal:	Maybe

ADV180003						
					N/A Vector: N/A	
Microsoft Office 2016 (32-bit edition)	4011622 Security Update	None	Defense in Depth	4011038	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011622 Security Update	None	Defense in Depth	4011038	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	None	Defense in Depth	4011038	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	None	Defense in Depth	4011038	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2018-0741 - Microsoft Color Management Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0741 MITRE NVD	**CVE Title:** Microsoft Color Management Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Color Management Module (ICM32.dll) handles objects in memory. This vulnerability allows an attacker to retrieve information to bypass usermode ASLR (Address Space Layout Randomization) on a targeted system. By itself, the information disclosure does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Color Management Module handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0741						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	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	4056894 Monthly	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5	Yes

CVE-2018-0741						
2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4056897 Security Only				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	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0741						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4056942 Security Update	Important	Information Disclosure	4054518	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	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056942 Security Update	Important	Information Disclosure	4054518	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	Unknown
Windows Server 2008 for 32-bit Systems	4056942 Security Update	Important	Information Disclosure	4054518	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	Unknown

CVE-2018-0741						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4056942 Security Update	Important	Information Disclosure	4054518	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	Unknown
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4056942 Security Update	Important	Information Disclosure	4054518	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	Unknown

CVE-2018-0743 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0743 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0743						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0743						
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056892 Security	Important	Elevation of Privilege	4054517	Base: 7 Temporal: 6.3	Yes

CVE-2018-0743						
1709 (Server Core Installation)	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	

CVE-2018-0744 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0744 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0744						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0744						
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0744						
Windows 10 for x64-based Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0744						
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056892 Security	Important	Elevation of Privilege	4054517	Base: 7 Temporal: 6.3	Yes

CVE-2018-0744						
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 1709 for x64-based Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0745 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0745 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0745						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for	4056891 Security	Important	Information Disclosure	4053580	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0745						
32-bit 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 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0745						
Installation)						

CVE-2018-0746 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0746 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0746						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4056896 Monthly Rollup 4056899 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0746						
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0746						
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056893 Security Update	Important	Information Disclosure	4053581	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056890 Security	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0746						
	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	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056891 Security	Important	Information Disclosure	4053580	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0746						
32-bit 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 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0747 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0747						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4056894 Monthly Rollup	Important	Information Disclosure	4054518	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0747						
Service Pack 1	4056897 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 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056613 Security	Important	Information Disclosure	4054518	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0747						
32-bit Systems Service Pack 2 (Server Core installation)	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 2012	4056896 Monthly Rollup 4056899 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747						
	Only					
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4056898 Security Only	Important	Information Disclosure	4054520	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747						
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056893 Security Update	Important	Information Disclosure	4053581	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056890 Security	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0747						
	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	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056891 Security Update	Important	Information Disclosure	4053580	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747						
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056613 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056613 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4056613 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0747						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4056613 Security Update	Important	Information Disclosure	4054517	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0748 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Kernel API enforces permissions. An attacker who successfully exploited the vulnerability could	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	impersonate processes, interject cross-process communication, or interrupt system functionality. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly enforces permissions. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability. 1.0 01/03/2018 08:00:00		

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-2018-0748						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4056615 Security Update	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4056896 Monthly Rollup 4056899 Security	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
	Only					
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Windows Server 2016	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based	4056615 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Systems Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2	4056615 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4056615 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4056615 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0748						
Core installation)						

CVE-2018-0749 - SMB Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0749 MITRE NVD	**CVE Title:** SMB Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine. An attacker who successfully exploited this vulnerability could bypass certain security checks in the operating system. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how Windows SMB Server handles such specially crafted files.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0749						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0749						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4056759 Security Update	Important	Elevation of Privilege	4054518	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0749						
Core installation)						
Windows Server 2012	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-	4056898 Security	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9	Yes

CVE-2018-0749						
based systems	Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0749						
x64-based Systems						
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0749						
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0749						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056759 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4056759 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4056759 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4056759 Security	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9	Yes

CVE-2018-0749						
based Systems Service Pack 2 (Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	

CVE-2018-0750 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0750 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** A Win32k information disclosure vulnerability exists when the Windows GDI component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0750						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	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	4056894 Monthly	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5	Yes

CVE-2018-0750						
2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Rollup 4056897 Security Only				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	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0750						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4056944 Security Update	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056944 Security Update	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4056944 Security Update	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0750						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4056944 Security Update	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4056944 Security Update	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0751 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0751 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Kernel API enforces permissions. An attacker who successfully exploited the vulnerability could impersonate processes, interject cross-process communication, or interrupt system functionality. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly enforces permissions. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0751						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4056896 Monthly Rollup	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9	Yes

CVE-2018-0751						
	4056899 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0751						
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0751						
Windows Server 2016	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0751						
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0752 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0752 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Kernel API enforces permissions. An attacker who successfully exploited the vulnerability could impersonate processes, interject cross-process communication, or interrupt system functionality. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by helping to ensure that the Windows Kernel API properly enforces permissions. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0752						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4056896 Monthly Rollup	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9	Yes

CVE-2018-0752						
	4056899 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0752						
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Elevation of Privilege	4054520	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0752						
Windows Server 2016	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0752						
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 6.6 Temporal: 5.9 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0753 - Windows IPSec Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0753 MITRE NVD	**CVE Title:** Windows IPSec Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in the way that Windows handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. Note that the denial of service condition would not allow an attacker to execute code or to elevate user privileges. However, the denial of service condition could prevent authorized users from using system resources. The security update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0753						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4056896 Monthly Rollup	Important	Denial of Service	4054520	Base: 5.9 Temporal: 5.3	Yes

CVE-2018-0753						
	4056899 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Denial of Service	4054520	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Denial of Service	4054520	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4056898 Security Only	Important	Denial of Service	4054520	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4056898 Security Only	Important	Denial of Service	4054520	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0753						
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Denial of Service	4054520	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Denial of Service	4053581	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4056893 Security Update	Important	Denial of Service	4053581	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Denial of Service	4053578	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Denial of Service	4053578	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0753						
Windows Server 2016	4056890 Security Update	Important	Denial of Service	4053579	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Denial of Service	4053579	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Denial of Service	4053579	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Denial of Service	4053579	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Denial of Service	4053580	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0753						
Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Denial of Service	4053580	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Denial of Service	4054517	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Denial of Service	4054517	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0754 - OpenType Font Driver Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0754 MITRE NVD	**CVE Title:** OpenType Font Driver Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. To exploit this vulnerability, an attacker would have to log on to an affected system and open a document containing specially crafted fonts. The update addresses the vulnerability by correcting how ATMFD.dll handles objects in memory. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0754						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0754						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4056941 Security Update	Important	Information Disclosure	4054518	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0754						
Service Pack 2 (Server Core installation)						
Windows Server 2012	4056896 Monthly Rollup 4056899 Security Only	Important	Information Disclosure	4054520	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Information Disclosure	4054520	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4056898 Security Only	Important	Information Disclosure	4054520	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2018-0754						
					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	
Windows 8.1 for x64-based systems	4056898 Security Only	Important	Information Disclosure	4054520	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4056898 Security Only	Important	Information Disclosure	4054520	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4056898 Security Only	Important	Information Disclosure	4054520	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0754						
Windows 10 for x64-based Systems	4056893 Security Update	Important	Information Disclosure	4053581	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 1511 for x64-based Systems	4056888 Security Update	Important	Information Disclosure	4053578	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 1511 for 32-bit Systems	4056888 Security Update	Important	Information Disclosure	4053578	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	4056890 Security Update	Important	Information Disclosure	4053579	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	4056890 Security	Important	Information Disclosure	4053579	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2018-0754						
32-bit Systems	Update				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	
Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Information Disclosure	4053579	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)	4056890 Security Update	Important	Information Disclosure	4053579	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Information Disclosure	4053580	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	4056891 Security Update	Important	Information Disclosure	4053580	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0754						
Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Information Disclosure	4054517	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056941 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0754						
Windows Server 2008 for 32-bit Systems Service Pack 2	4056941 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4056941 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4056941 Security Update	Important	Information Disclosure	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0754						
Core installation)						

CVE-2018-0758 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0758 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0758						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0758						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4056890 Security Update	Moderate	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4056890 Security	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0758						
10 Version 1607 for x64-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 1703 for 32-bit Systems	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0758						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0762 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0762 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:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0762						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0762						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	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	4056894 Monthly Rollup	Critical	Remote Code	4052978	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2018-0762						
Windows 7 for 32-bit Systems Service Pack 1	4056568 IE Cumulative		Execution		CVSS: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	4056894 Monthly Rollup 4056568 IE Cumulative	Critical	Remote Code Execution	4052978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056894 Monthly Rollup 4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4056895 Monthly Rollup 4056568 IE Cumulative	Critical	Remote Code Execution	4052978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056895 Monthly Rollup 4056568 IE Cumulative	Critical	Remote Code Execution	4052978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056895 Monthly Rollup 4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
Internet Explorer 11 on Windows RT 8.1	4056895 Monthly Rollup	Critical	Remote Code Execution	4054519	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056890 Security Update	Moderate	Remote Code Execution	4053579	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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056896 Monthly Rollup 4056568 IE	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector:	Yes

CVE-2018-0762						
Server 2012	Cumulative				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	
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4056888 Security	Critical	Remote Code	4053578	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0762						
Windows 10 Version 1511 for 32-bit 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	4056890 Security Update	Moderate	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0762						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0764 - .NET and .NET Core Denial Of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0764	**CVE Title:** .NET and .NET Core Denial Of Service Vulnerability **Description:** A Denial of Service vulnerability exists when .NET, and .NET core, improperly process XML documents. An attacker who successfully exploited this vulnerability could cause a	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	denial of service against a .NET application. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to a .NET(or .NET core) application. The update addresses the vulnerability by correcting how a .NET, and .NET core, applications handles XML document processing. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0764						
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	4054995 Monthly Rollup 4054172 Security Only	Important	Denial of Service	3122656	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	4054995 Monthly Rollup 4054172 Security Only	Important	Denial of Service	3122656	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)	4054995 Monthly Rollup 4054172	Important	Denial of Service	3122656	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0764						
	Security Only					
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4054995 Monthly Rollup 4054172 Security Only	Important	Denial of Service	3122656	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4054994 Monthly Rollup 4054171 Security Only	Important	Denial of Service	3122655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4054994 Monthly Rollup 4054171 Security Only	Important	Denial of Service	3122655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4054993 Monthly Rollup	Important	Denial of Service	3122654	Base: N/A Temporal:	Maybe

CVE-2018-0764						
	4054170 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4054170 Security Only 4054993 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4054170 Security Only 4054993 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4054993 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4054170 Security Only 4054993 Monthly	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0764						
	Rollup					
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2	4054172 Security Only 4054995 Monthly Rollup	Important	Denial of Service	4049017, 4041086	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	4054172 Security Only 4054995 Monthly Rollup	Important	Denial of Service	4049017, 4041086	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Denial of Service	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems	4056893 Security Update	Important	Denial of Service	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0764						
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4054183 Security Only 4055002 Monthly Rollup	Important	Denial of Service	4049019, 4041086	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	4055002 Monthly Rollup 4054183 Security Only	Important	Denial of Service	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Denial of Service	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Denial of Service	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems	4056891 Security	Important	Denial of Service	4053580	Base: N/A Temporal:	Yes

CVE-2018-0764						
	Update				N/A Vector: N/A	
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Denial of Service	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0764						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for 32-bit Systems Service Pack 1	4055002 Monthly Rollup 4054183 Security Only	Important	Denial of Service	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for x64-based Systems Service Pack 1	4055002 Monthly Rollup 4054183 Security Only	Important	Denial of Service	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4055002 Monthly Rollup 4054183 Security Only	Important	Denial of Service	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4055002 Monthly Rollup 4054183	Important	Denial of Service	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0764						
	Security Only					
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012	4055000 Monthly Rollup 4054181 Security Only	Important	Denial of Service	3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 (Server Core installation)	4055000 Monthly Rollup 4054181 Security Only	Important	Denial of Service	3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for 32-bit systems	4054182 Security Only 4055001 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for x64-based systems	4054182 Security Only 4055001	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal:	Maybe

CVE-2018-0764						
	Monthly Rollup				N/A Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2	4054182 Security Only 4055001 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows RT 8.1	4055001 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2 (Server Core installation)	4054182 Security Only 4055001 Monthly Rollup	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core 1.0	Commit Security Update	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0764						
.NET Core 1.1	Commit Security Update	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.0	Commit Security Update	Important	Denial of Service	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Denial of Service	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Denial of Service	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1 on Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Denial of Service	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2012	4054997 Monthly Rollup	Important	Denial of Service	3122655, 3122658	Base: N/A Temporal:	Maybe

CVE-2018-0764						
	4054175 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4054997 Monthly Rollup 4054175 Security Only	Important	Denial of Service	3122655, 3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4054999 Monthly Rollup 4054177 Security Only	Important	Denial of Service	3122651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4054999 Monthly Rollup 4054177 Security Only	Important	Denial of Service	3122651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4054999 Monthly	Important	Denial of Service	3122651	Base: N/A Temporal:	Maybe

CVE-2018-0764						
	Rollup 4054177 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4054999 Monthly Rollup 4054177 Security Only	Important	Denial of Service	3122651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Denial of Service	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4056893 Security Update	Important	Denial of Service	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Denial of Service	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0764						
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Denial of Service	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Denial of Service	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4056891 Security	Important	Denial of Service	4053580	Base: N/A Temporal:	Yes

CVE-2018-0764						
	Update				N/A Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Denial of Service	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4054996 Monthly Rollup 4054174 Security Update	Important	Denial of Service	3122646	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	4054996 Monthly Rollup 4054174 Security Only	Important	Denial of Service	3122646	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	4054996 Monthly Rollup 4054174	Important	Denial of Service	3122646	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0764						
	Security Only					
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4054996 Monthly Rollup 4054174 Security Update	Important	Denial of Service	3122646	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	4054996 Monthly Rollup 4054174 Security Only	Important	Denial of Service	3122646	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	4054996 Monthly Rollup 4054174 Security Only	Important	Denial of Service	3122646	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	4054998 Monthly	Important	Denial of Service	2973112, 3122648	Base: N/A Temporal:	Maybe

CVE-2018-0764						
	Rollup 4054176 Security Only				N/A Vector: N/A	
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1	4054998 Monthly Rollup 4054176 Security Only	Important	Denial of Service	2973112, 3122648	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)	4054998 Monthly Rollup 4054176 Security Only	Important	Denial of Service	2973112, 3122648	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	4054998 Monthly Rollup 4054176 Security Only	Important	Denial of Service	2973112, 3122648	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0764						
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4054998 Monthly Rollup 4054176 Security Only	Important	Denial of Service	2973112, 3122648	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0766 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0766 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that contains malicious PDF content. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted PDF content that could exploit the vulnerability. However, in all cases an attacker would have	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Microsoft Edge PDF Reader handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0766						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4056893 Security Update	Important	Information Disclosure	4053581	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4056888 Security	Important	Information Disclosure	4053578	Base: 4.3 Temporal: 3.9	Yes

CVE-2018-0766						
10 Version 1511 for x64-based Systems	Update				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	
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Information Disclosure	4053578	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4056890 Security Update	Low	Information Disclosure	4053579	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0766						
Version 1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Information Disclosure	4053579	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Information Disclosure	4053580	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4056891 Security	Important	Information Disclosure	4053580	Base: 4.3 Temporal: 3.9	Yes

CVE-2018-0766						
Windows 10 Version 1703 for x64-based Systems	Update				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	
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-	4056892 Security Update	Important	Information Disclosure	4054517	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0766						
based Systems						

CVE-2018-0767 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0767 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user	Critical	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0767						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Information Disclosure	4053578	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Information Disclosure	4053578	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0767						
Microsoft Edge on Windows Server 2016	4056890 Security Update	Moderate	Information Disclosure	4053579	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Critical	Information Disclosure	4053579	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Critical	Information Disclosure	4053579	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4056891 Security	Critical	Information Disclosure	4053580	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0767						
1703 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	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Critical	Information Disclosure	4053580	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Information Disclosure	4054517	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4056892 Security Update	Critical	Information Disclosure	4054517	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0767						
x64-based Systems						
ChakraCore	Commit Security Update	Critical	Information Disclosure	4054517	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0768 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0768 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revised the Affected Products table to include ChakraCore for this vulnerability.		

Affected Software

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

CVE-2018-0768						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0768						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Important	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0769 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0769	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0769						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0769						
Microsoft Edge on Windows 10 for x64-based Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4056890 Security	Moderate	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0769						
Windows Server 2016	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 32-bit Systems	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0769						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0769						
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0770 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0770 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0770						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0770						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4056890 Security Update	Moderate	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4056890 Security	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0770						
10 Version 1607 for x64-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 1703 for 32-bit Systems	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0770						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0772 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0772 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:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0772						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0772						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	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	4056894 Monthly Rollup	Critical	Remote Code	4052978	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2018-0772						
Windows 7 for 32-bit Systems Service Pack 1	4056568 IE Cumulative		Execution		CVSS: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	4056894 Monthly Rollup 4056568 IE Cumulative	Critical	Remote Code Execution	4052978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056894 Monthly Rollup 4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4056895 Monthly Rollup 4056568 IE Cumulative	Critical	Remote Code Execution	4052978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056895 Monthly Rollup 4056568 IE Cumulative	Critical	Remote Code Execution	4052978	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056895 Monthly Rollup 4056568 IE Cumulative	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
Internet Explorer 11 on Windows RT 8.1	4056895 Monthly Rollup	Critical	Remote Code Execution	4054519	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056890 Security Update	Moderate	Remote Code Execution	4053579	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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/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	4056896 Monthly Rollup 4056568 IE	Moderate	Remote Code Execution	4052978	Base: 6.4 Temporal: 5.8 Vector:	Yes

CVE-2018-0772						
Server 2012	Cumulative				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	
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4056888 Security	Critical	Remote Code	4053578	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0772						
Windows 10 Version 1511 for 32-bit 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	4056890 Security Update	Moderate	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0772						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0773 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0773	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0773						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0773						
1709 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0774 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0774 MITRE NVD	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0774						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10	4056892 Security	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0774						
Version 1709 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 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0775 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0775 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability.		

Affected Software

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

CVE-2018-0775						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0776 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0776 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0776						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/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	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4056888 Security	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0776						
10 Version 1511 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 Server 2016	4056890 Security Update	Moderate	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0776						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0776						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0777 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0777	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory	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 scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability.		

Affected Software

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

CVE-2018-0777						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0777						
Microsoft Edge on Windows 10 for x64-based Systems	4056893 Security Update	Critical	Remote Code Execution	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0777						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0777						
1703 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0778 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0778 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0778						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0780 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0780 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:**	Critical	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0780						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Critical	Information Disclosure	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/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	4056893 Security Update	Critical	Information Disclosure	4053581	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Information Disclosure	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0780						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Information Disclosure	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4056890 Security Update	Moderate	Information Disclosure	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056890 Security Update	Critical	Information Disclosure	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4056890 Security	Critical	Information Disclosure	4053579	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0780						
1607 for x64-based Systems	Update				CVSS: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 32-bit Systems	4056891 Security Update	Critical	Information Disclosure	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Information Disclosure	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Information Disclosure	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0780						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Information Disclosure	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Information Disclosure	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0781 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0781 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability.		

Affected Software

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

CVE-2018-0781						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Critical	Remote Code Execution	4053578	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0781						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Critical	Remote Code Execution	4053579	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056891 Security Update	Critical	Remote Code Execution	4053580	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0781						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4056892 Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Remote Code Execution	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0784 - ASP.NET Core Elevation Of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0784 MITRE NVD	**CVE Title:** ASP.NET Core Elevation Of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when a ASP.NET Core web application, created using vulnerable project templates, fails to properly sanitize web requests. An attacker who successfully exploited this vulnerability could perform content injection attacks and run script in the security context of the logged-on user. To exploit the vulnerability, an attacker could send a specially crafted email, containing a malicious link, to a user. Alternatively, an attacker could use a chat client to social engineer a user into clicking the malicious link. However, in all cases to exploit this vulnerability a user must click a maliciously crafted link from an attacker. The security update addresses the vulnerability by correcting the ASP.NET Core project templates. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0784						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.0	Commit Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0784						
ASP.NET Core 2.0 on Windows 10 Version 1703 for 32-bit Systems	Commit Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0785 - ASP.NET Core Cross Site Request Forgery Vulnerabilty

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0785 MITRE NVD	**CVE Title:** ASP.NET Core Cross Site Request Forgery Vulnerabilty **Description:** A Cross Site Request Forgery (CSRF) vulnerability exists when a ASP.NET Core web application is created using vulnerable project templates. An attacker who successfully exploited this vulnerability could change the recovery codes associated with the victim's user account without his/her consent. As a result, a victim of this attack may be permanently locked out of his/her account after loosing access to his/her 2FA device, as the initial recovery codes would be no longer valid. The update corrects the ASP.NET Core project templates.	Moderate	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **What does the update do?** The update corrects the project templates for ####. The template updates only affect new applications. For this reason, Microsoft strongly recommends that developers who have built web applications using these templates take immediate action to evaluate their web applications for exposure to the vulnerability, and then use the workarounds in the Suggested Actions section to make code changes to update their applications to protect them from the vulnerability. If you are running Visual Studio 2013, you need to use the workaround steps listed in the Suggested Actions section to update your applications manually every time you use the affected templates. **How do I apply the update?** 1. Start Visual Studio. 2. Under the Tools menu, choose Extensions and Updates. 3. Expand the Updates tree. 4. Under Product Updates locate the following two entries: â€¢ Microsoft ASP.NET and Web Tools â€¢ Microsoft ASP.NET Web Frameworks and Tools 5. Select each update and click Update.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Suggested Actions The following workaround information details the changes that you must make to existing applications created from the ASP.NET project templates. Visual Studio 2015 MVC 5 and Visual Studio 2013 MVC 5 For C# **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0785						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0785						
ASP.NET Core 2.0	Commit Security Update	Moderate	Tampering		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0786 - .NET Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0786 MITRE NVD	**CVE Title:** .NET Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft .NET Framework (and .NET Core) components do not completely validate certificates. An attacker could present a certificate that is marked invalid for a specific use, but the component uses it for that purpose. This action disregards the Enhanced Key Usage taggings. The security update addresses the vulnerability by helping to ensure that .NET Framework (and .NET Core) components completely validate certificates. **FAQ:** None	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0786						
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	4054995 Monthly Rollup 4054172	Important	Security Feature Bypass	3122656	Base: N/A Temporal: N/A	Maybe

CVE-2018-0786						
	Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1	4054995 Monthly Rollup 4054172 Security Only	Important	Security Feature Bypass	3122656	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)	4054995 Monthly Rollup 4054172 Security Only	Important	Security Feature Bypass	3122656	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	4054995 Monthly Rollup 4054172 Security Only	Important	Security Feature Bypass	3122656	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012	4054994 Monthly Rollup	Important	Security Feature Bypass	3122655	Base: N/A Temporal: N/A	Maybe

CVE-2018-0786						
	4054171 Security Only				Vector: N/A	
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)	4054994 Monthly Rollup 4054171 Security Only	Important	Security Feature Bypass	3122655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems	4054993 Monthly Rollup 4054170 Security Only	Important	Security Feature Bypass	3122654	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems	4054170 Security Only 4054993 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2	4054170 Security Only 4054993 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows RT 8.1	4054993 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)	4054170 Security Only 4054993 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	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	4054172 Security Only 4054995 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041086	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2	4054172 Security Only 4054995 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041086	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Security Feature Bypass	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems	4056893 Security Update	Important	Security Feature Bypass	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2	4054183 Security Only 4055002 Monthly Rollup	Important	Security Feature Bypass	4049019, 4041086	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2	4055002 Monthly Rollup 4054183 Security Only	Important	Security Feature Bypass	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Security Feature Bypass	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Security Feature Bypass	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Security Feature Bypass	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0786						
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Security Feature Bypass	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016 (Server Core installation)	4056890 Security	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A	Yes

CVE-2018-0786						
	Update				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for 32-bit Systems Service Pack 1	4055002 Monthly Rollup 4054183 Security Only	Important	Security Feature Bypass	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for x64-based Systems Service Pack 1	4055002 Monthly Rollup 4054183 Security Only	Important	Security Feature Bypass	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4055002 Monthly Rollup 4054183 Security Only	Important	Security Feature Bypass	3122661	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4055002 Monthly Rollup	Important	Security Feature Bypass	3122661	Base: N/A Temporal: N/A	Maybe

CVE-2018-0786						
	4054183 Security Only				Vector: N/A	
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012	4055000 Monthly Rollup 4054181 Security Only	Important	Security Feature Bypass	3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 (Server Core installation)	4055000 Monthly Rollup 4054181 Security Only	Important	Security Feature Bypass	3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for 32-bit systems	4054182 Security Only 4055001 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for x64-based systems	4054182 Security Only 4055001 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2	4054182 Security Only 4055001 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows RT 8.1	4055001 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2 (Server Core installation)	4054182 Security Only 4055001 Monthly Rollup	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
.NET Core 1.0	Commit Security Update	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.0	Commit Security Update	Important	Security Feature Bypass	4049017, 4041085	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Important	Security Feature Bypass	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Security Feature Bypass	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 4.7.1 on Windows Server, version 1709 (Server Core Installation)	4056892 Security	Important	Security Feature Bypass	4054517	Base: N/A Temporal: N/A	Yes

CVE-2018-0786						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012	4054997 Monthly Rollup 4054175 Security Only	Important	Security Feature Bypass	3122655, 3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)	4054997 Monthly Rollup 4054175 Security Only	Important	Security Feature Bypass	3122655, 3122658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems	4054999 Monthly Rollup 4054177 Security Only	Important	Security Feature Bypass	3122651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems	4054999 Monthly Rollup	Important	Security Feature Bypass	3122660	Base: N/A Temporal: N/A	Maybe

CVE-2018-0786						
	4054182 Security Only				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows Server 2012 R2	4054999 Monthly Rollup 4054177 Security Only	Important	Security Feature Bypass	3122651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)	4054999 Monthly Rollup 4054177 Security Only	Important	Security Feature Bypass	3122651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Security Feature Bypass	4053581	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems	4056893 Security	Important	Security Feature Bypass	4053581	Base: N/A Temporal: N/A	Yes

CVE-2018-0786						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Security Feature Bypass	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Security Feature Bypass	4053578	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0786						
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)	4056890 Security Update	Important	Security Feature Bypass	4053579	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Security Feature Bypass	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Security Feature Bypass	4053580	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems	4056892 Security	Important	Security Feature Bypass	4054517	Base: N/A Temporal: N/A	Yes

CVE-2018-0786						
	Update				Vector: N/A	
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Security Feature Bypass	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.5 on Windows Server, version 1709 (Server Core Installation)	4056892 Security Update	Important	Security Feature Bypass	4054517	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2	4054996 Monthly Rollup 4054174 Security Update	Important	Security Feature Bypass	3122646	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	4054996 Monthly Rollup 4054174	Important	Security Feature Bypass	3122646	Base: N/A Temporal: N/A	Maybe

CVE-2018-0786						
	Security Only				Vector: N/A	
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4054996 Monthly Rollup 4054174 Security Only	Important	Security Feature Bypass	3122646	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	4054996 Monthly Rollup 4054174 Security Update	Important	Security Feature Bypass	3122646	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	4054996 Monthly Rollup 4054174 Security Only	Important	Security Feature Bypass	3122646	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2	4054996 Monthly Rollup 4054174 Security Only	Important	Security Feature Bypass	3122646	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	4054998 Monthly Rollup 4054176 Security Only	Important	Security Feature Bypass	2973112, 3122648	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	4054998 Monthly Rollup 4054176 Security Only	Important	Security Feature Bypass	2973112, 3122648	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)	4054998 Monthly Rollup 4054176	Important	Security Feature Bypass	2973112, 3122648	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0786						
	Security Only					
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4054998 Monthly Rollup 4054176 Security Only	Important	Security Feature Bypass	2973112, 3122648	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	4054998 Monthly Rollup 4054176 Security Only	Important	Security Feature Bypass	2973112, 3122648	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0788 - OpenType Font Driver Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0788 MITRE NVD	**CVE Title:** OpenType Font Driver Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code and take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability, an attacker would first have to log on to a target system and then run a specially crafted application. The security update addresses the vulnerability by correcting how ATMFD.dll handles objects in memory. **FAQ:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published. 2.0 01/05/2018 08:00:00 Revised the Affected Products table to add Monthly Rollup updates for Windows 7, Windows Server 2008 R2, and Windows Server 2012. Customers who install Monthly Rollups should install these updates to be protected from this vulnerability.		

Affected Software

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

CVE-2018-0788						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0788						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4056894 Monthly Rollup 4056897 Security Only	Important	Information Disclosure	4054518	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4056894 Monthly	Important	Information Disclosure	4054518	Base: 7 Temporal: 6.3 Vector:	Yes

CVE-2018-0788						
x64-based Systems Service Pack 1	Rollup 4056897 Security Only				CVSS: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 Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4056941 Security Update	Important	Information Disclosure	4054518	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056896 Monthly Rollup 4056899	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0788						
	Security Only					
Windows Server 2012 (Server Core installation)	4056896 Monthly Rollup 4056899 Security Only	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056898 Security Only	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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	4056898 Security Only	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0788						
Windows Server 2012 R2	4056898 Security Only	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/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)	4056898 Security Only	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056941 Security Update	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4056941 Security	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector:	Yes

CVE-2018-0788						
32-bit Systems Service Pack 2	Update				CVSS: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 Server 2008 for x64-based Systems Service Pack 2	4056941 Security Update	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4056941 Security Update	Important	Information Disclosure	4054520	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0789 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0789 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	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0789						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0789						
Microsoft SharePoint Server 2010 Service Pack 2	3114998 Security Update	Important	Spoofing	2956077	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011642 Security Update	Important	Spoofing	4011576	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011653 Security Update	Important	Spoofing	4011180	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0790 - Microsoft SharePoint Cross Site Scripting Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0790 MITRE NVD	**CVE Title:** Microsoft SharePoint Cross Site Scripting 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	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0790						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0790						
Microsoft SharePoint Foundation 2010 Service Pack 2	3141547 Security Update	Important	Information Disclosure	3114890	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011642 Security Update	Important	Information Disclosure	4011576	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011653 Security Update	Important	Information Disclosure	4011180	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0791 - Microsoft Outlook Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0791 MITRE NVD	**CVE Title:** Microsoft Outlook Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft Outlook parses specially crafted email messages. 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. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Outlook. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file. The security update addresses the vulnerability by correcting the way that Microsoft Outlook parses specially crafted email messages. **FAQ:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0791						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0791						
Microsoft Outlook 2007 Service Pack 3	4011213 Security Update	Important	Remote Code Execution	4011110	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 RT Service Pack 1	4011637 Security Update	Important	Remote Code Execution	4011178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2010 Service Pack 2 (32-bit editions)	4011273 Security Update	Important	Remote Code Execution	4011196	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2010 Service Pack 2 (64-bit editions)	4011273 Security Update	Important	Remote Code Execution	4011196	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (32-bit edition)	4011626 Security Update	Important	Remote Code Execution	4011162	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2016 (64-bit edition)	4011626 Security Update	Important	Remote Code Execution	4011162	Base: N/A Temporal:	Maybe

CVE-2018-0791						
					N/A Vector: N/A	
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)	4011637 Security Update	Important	Remote Code Execution	4011178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)	4011637 Security Update	Important	Remote Code Execution	4011178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011178	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2018-0792 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0792 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0792						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Online Server 2016	4011021 Security Update	Important	Remote Code Execution	4011020	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011020	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0792						
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011020	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft SharePoint Enterprise Server 2016	4011642 Security Update	Important	Remote Code Execution	4011576	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0793 - Microsoft Outlook Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0793 MITRE NVD	**CVE Title:** Microsoft Outlook Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft Outlook parses specially crafted email messages. An attacker who successfully exploited the	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Outlook. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file. The security update addresses the vulnerability by correcting the way that Microsoft Outlook parses specially crafted email messages. **FAQ:** **I have Microsoft Word 2010 installed. Why am I not being offered the 4011658 update?** The 4011658 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update. **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?** When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	considered to be applicable to all supported products and versions that contain the vulnerable component. For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table. For more information on this behavior and recommended actions, see Microsoft Knowledge Base Article 830335. For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update. **Why is there a separate update for Word Viewer** The Word Viewer update (4011641) is only supported, and will only install from Microsoft Update, if itâ€™s on Windows Embedded POSReady 2009. This is because Word Viewer ships pre-installed in		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Windows Embedded POSReady 2009, which is still in support. For other platforms, Word Viewer is no longer supported. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0793						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0793						
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011658 Security Update	Important	Remote Code Execution	4011612	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011658 Security Update	Important	Remote Code Execution	4011612	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal:	Maybe

CVE-2018-0793						
					N/A Vector: N/A	
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0793						
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0794 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0794 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** **I have Microsoft Word 2010 installed. Why am I not being offered the 4011658 update?** The 4011658 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update? When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component. For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table. For more information on this behavior and recommended actions, see Microsoft Knowledge Base Article 830335. For a list of Microsoft Office products that an update		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update. **Why is there a separate update for Word Viewer** The Word Viewer update (4011641) is only supported, and will only install from Microsoft Update, if itâ€™s on Windows Embedded POSReady 2009. This is because Word Viewer ships pre-installed in Windows Embedded POSReady 2009, which is still in support. For other platforms, Word Viewer is no longer supported. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0794						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011658 Security Update	Important	Remote Code Execution	4011612	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0794						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011658 Security Update	Important	Remote Code Execution	4011612	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal:	Maybe

CVE-2018-0794						
					N/A Vector: N/A	
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0795 - Microsoft Office Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0795 MITRE NVD	**CVE Title:** Microsoft Office Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0795						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011611 Security Update	Important	Remote Code Execution	4011055	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011611 Security Update	Important	Remote Code Execution	4011055	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011636 Security Update	Important	Remote Code Execution	4011103	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011636 Security Update	Important	Remote Code Execution	4011103	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	4011636 Security Update	Important	Remote Code Execution	4011103	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0795						
Microsoft Office 2016 (32-bit edition)	4011632 Security Update	Important	Remote Code Execution	3191944	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011632 Security Update	Important	Remote Code Execution	3191944	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	3191944	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	3191944	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2018-0796 - Microsoft Excel Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0796 MITRE NVD	**CVE Title:** Microsoft Excel Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0796						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2007 Service Pack 3	4011602 Security Update	Important	Remote Code Execution	4011199	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel Viewer 2007 Service Pack 3	4011606 Security Update	Important	Remote Code Execution	4011206	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4011660 Security Update	Important	Remote Code Execution	4011197	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4011660 Security Update	Important	Remote Code Execution	4011197	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4011639 Security Update	Important	Remote Code Execution	4011233	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0796						
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4011639 Security Update	Important	Remote Code Execution	4011233	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4011639 Security Update	Important	Remote Code Execution	4011233	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (32-bit edition)	4011627 Security Update	Important	Remote Code Execution	4011220	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4011627 Security Update	Important	Remote Code Execution	4011220	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011220	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011220	Base: N/A Temporal:	No

CVE-2018-0796						
					N/A Vector: N/A	
Microsoft Office Compatibility Pack Service Pack 3	4011605 Security Update	Important	Remote Code Execution	4011205	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0797 - Microsoft Word Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0797 MITRE NVD	**CVE Title:** Microsoft Word Memory Corruption Vulnerability **Description:** An Office RTF remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle RTF files. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office 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 designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by changing the way Microsoft Office software handles RTF content. **FAQ:** **I have Microsoft Word 2010 installed. Why am I not being offered the 4011658 update?** The 4011658 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update. **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table.**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Why am I being offered this update? When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component. For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table. For more information on this behavior and recommended actions, see Microsoft Knowledge Base Article 830335. For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Why is there a separate update for Word Viewer The Word Viewer update (4011641) is only supported, and will only install from Microsoft Update, if itâ€™s on Windows Embedded POSReady 2009. This is because Word Viewer ships pre-installed in Windows Embedded POSReady 2009, which is still in support. For other platforms, Word Viewer is no longer supported. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0797						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Critical	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2010 Service Pack 2	4011609 Security Update	Critical	Remote Code Execution	4011267	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Critical	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Critical	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011658 Security Update	Critical	Remote Code Execution	4011612	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0797						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011658 Security Update	Critical	Remote Code Execution	4011612	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	4011615 Security Update	Critical	Remote Code Execution	4011271	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Critical	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Critical	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Critical	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps Server 2013 Service Pack 1	4011648 Security Update	Critical	Remote Code Execution	4011247	Base: N/A Temporal:	Maybe

CVE-2018-0797						
					N/A Vector: N/A	
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Remote Code Execution	4011247	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Critical	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Critical	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Online Server 2016	4011021 Security Update	Critical	Remote Code Execution	4011020	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011642 Security Update	Critical	Remote Code Execution	4011576	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0797						
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011579 Security Update	Critical	Remote Code Execution	4011245	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4011641 Security Update	Critical	Remote Code Execution	4011245	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Critical	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0798 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0798	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0798						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0798						
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal:	Maybe

CVE-2018-0798						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0798						
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal:	Maybe

CVE-2018-0798						
					N/A Vector: N/A	

CVE-2018-0799 - Microsoft Access Tampering Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0799 MITRE NVD	**CVE Title:** Microsoft Access Tampering Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft Access does not properly sanitize inputs to image fields edited within Design view. An attacker could exploit the vulnerability by sending a specially crafted file to a victim, or by hosting the file on a web server. The attacker who successfully exploited the vulnerability could then run javascript 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 a remote site on behalf of the user, and inject malicious content in the browser of the user.	Important	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by helping to ensure that Microsoft Access properly sanitizes image field values. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0799						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4011642 Security Update	Important	Tampering	4011576	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011599 Security Update	Important	Tampering	3178633	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0800 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0800 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully	Critical	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	exploited the vulnerability could obtain information to further compromise the userâ€™s system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revised the Affected Products table to include ChakraCore for this vulnerability. 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0800						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4056892 Security Update	Critical	Information Disclosure	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0800						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Critical	Information Disclosure	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Update	Critical	Information Disclosure	4054517	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0801 - Microsoft Office Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0801	**CVE Title:** Microsoft Office Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882 **FAQ:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0801						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0801						
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal:	Maybe

CVE-2018-0801						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0801						
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal:	No

CVE-2018-0801						
					N/A Vector: N/A	
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0802 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0802 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882 **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0802						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0802						
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal:	Maybe

CVE-2018-0802						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0802						
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal:	Maybe

CVE-2018-0802						
					N/A Vector: N/A	

CVE-2018-0803 - Microsoft Edge Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0803 MITRE NVD	**CVE Title:** Microsoft Edge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to 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 users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action. For example, an attacker could trick users into clicking a link that takes	Low	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	them to the attacker's site. An attacker who successfully exploited this vulnerability could elevate privileges in affected versions of Microsoft Edge. The security update addresses the vulnerability by helping to ensure that cross-domain policies are properly enforced in Microsoft Edge. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0803						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4056893 Security Update	Important	Elevation of Privilege	4053581	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0803						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4056888 Security Update	Important	Elevation of Privilege	4053578	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4056890 Security Update	Low	Elevation of Privilege	4053579	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4056890 Security Update	Important	Elevation of Privilege	4053579	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0803						
1607 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4056891 Security Update	Important	Elevation of Privilege	4053580	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0803						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4056892 Security Update	Important	Elevation of Privilege	4054517	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0804 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0804 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take	Low	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882 **FAQ:** None **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0804						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Low	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0804						
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Low	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Low	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Low	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Low	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Low	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Low	Remote Code Execution	4011590	Base: N/A Temporal:	Maybe

CVE-2018-0804						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Low	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Low	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Low	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Low	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Low	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0804						
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Low	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Low	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Low	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Low	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Low	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Low	Remote Code Execution	4011265	Base: N/A Temporal:	Maybe

CVE-2018-0804						
					N/A Vector: N/A	

CVE-2018-0805 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0805 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882 **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0805						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0805						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal:	Maybe

CVE-2018-0805						
					N/A Vector: N/A	
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0805						
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0806 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0806	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0806						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0806						
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal:	Maybe

CVE-2018-0806						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0806						
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal:	No

CVE-2018-0806						
					N/A Vector: N/A	
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0807 - Microsoft Word Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0807 MITRE NVD	**CVE Title:** Microsoft Word Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882 **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0807						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0807						
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal:	Maybe

CVE-2018-0807						
					N/A Vector: N/A	
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011651 Security Update	Important	Remote Code Execution	4011590	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0807						
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal:	Maybe

CVE-2018-0807						
					N/A Vector: N/A	

CVE-2018-0812 - Microsoft Word Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0812 MITRE NVD	**CVE Title:** Microsoft Word Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by removing Equation Editor functionality. For more information on this change, please refer to the following article: https://support.microsoft.com/en-us/help/4057882 **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0812						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011656 Security Update	Important	Remote Code Execution	4011604	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2007 Service Pack 3	4011657 Security Update	Important	Remote Code Execution	4011608	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011659 Security Update	Important	Remote Code Execution	4011614	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0812						
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011610 Security Update	Important	Remote Code Execution	4011618	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal:	Maybe

CVE-2018-0812						
					N/A Vector: N/A	
Microsoft Word 2013 RT Service Pack 1	4011580 Security Update	Important	Remote Code Execution	3162047	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (32-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011643 Security Update	Important	Remote Code Execution	4011575	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011574 Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0812						
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	4011262	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office Compatibility Pack Service Pack 3	4011607 Security Update	Important	Remote Code Execution	4011265	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0818 - Scripting Engine Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0818	**CVE Title:** Scripting Engine Security Feature Bypass **Description:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A security feature bypass vulnerability exists in the Microsoft Chakra scripting engine that allows Control Flow Guard (CFG) to be bypassed. By itself, the CFG bypass vulnerability does not allow arbitrary code execution. However, an attacker could use the CFG bypass vulnerability in conjunction with another vulnerability, such as a remote code execution vulnerability, to run arbitrary code on a target system. To exploit the CFG bypass vulnerability, a user must be logged on to the Microsoft Chakra scripting engine and running it. The user would then need to browse to a malicious website. The security update addresses the CFG bypass vulnerability by helping to ensure that the Microsoft Chakra scripting engine properly handles accessing memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 2.0 01/05/2018 08:00:00 Revised the Affected Products table to include ChakraCore for this vulnerability.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 01/03/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0818						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ChakraCore	Commit Security Update	Important	Security Feature Bypass		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-2018-0819 - Spoofing Vulnerability in Microsoft Office for MAC

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0819 MITRE NVD	**CVE Title:** Spoofing Vulnerability in Microsoft Office for MAC **Description:** A spoofing vulnerability exists when Microsoft Outlook for MAC does not properly handle the encoding and display of email addresses. This improper handling and display may cause antivirus or antispam scanning to not work as intended. To exploit the vulnerability, an attacker could send a specially crafted email attachment to a user in an attempt to launch a social engineering attack, such as phishing. The security update addresses the vulnerability by correcting how Outlook for MAC displays encoded email addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 01/09/2018 08:00:00 Information published.		

Affected Software

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

CVE-2018-0819						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	No

声 明

==========

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

关于绿盟科技

==========

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

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

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

绿盟科技官方微博二维码

绿盟科技官方微信二维码