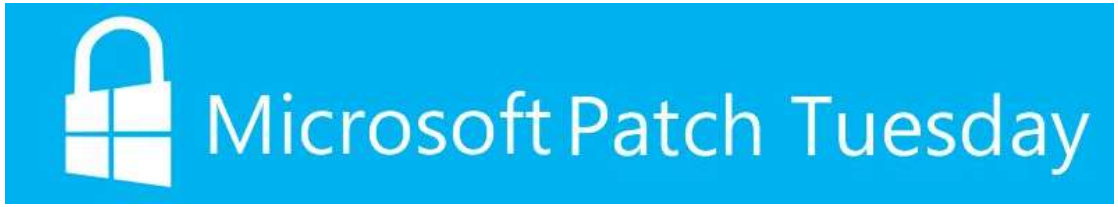
微软发布 8 月补丁修复 48 个安全问题

安全威胁通告



发布时间：2017 年 8 月 9 日

综述

微软于周二发布了 8 月安全更新补丁，修复了 48 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 Internet Explorer、Microsoft Edge、Microsoft Windows、Microsoft SharePoint、Microsoft SQL Server 以及 Adobe Flash Player。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE 编号	CVE 标题
Adobe Flash Player	ADV170010	August 2017 Flash Update

Common Log File System Driver（通用日志文件系统驱动）	CVE-2017-8624	Windows CLFS 特权漏洞提升
Internet Explorer	CVE-2017-8669	Microsoft 浏览器内存损坏漏洞
Internet Explorer	CVE-2017-8625	Internet Explorer 安全功能绕过
Internet Explorer	CVE-2017-8653	Microsoft 浏览器内存损坏漏洞
Internet Explorer	CVE-2017-8651	Internet 浏览器内存损坏漏洞
Microsoft Edge	CVE-2017-8503	Microsoft Edge 特权漏洞提升
Microsoft Edge	CVE-2017-8652	Microsoft Edge 信息泄露漏洞

Microsoft Edge	CVE-2017-8650	Microsoft Edge 安全功能绕过漏洞
Microsoft Edge	CVE-2017-8662	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-8661	Microsoft Edge 内存破坏漏洞
Microsoft Edge	CVE-2017-8642	Microsoft Edge 特权提升漏洞
Microsoft Edge	CVE-2017-8644	Microsoft Edge 信息泄露漏洞
Microsoft JET Database Engine（JET 数据库引擎）	CVE-2017-0250	Microsoft JET Database Engine 远程代码执行漏洞
Microsoft Office	CVE-2017-8654	Microsoft Office SharePoint XSS 漏洞

Microsoft Scripting Engine（脚本引擎）	CVE-2017-8656	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8655	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8657	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8641	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8645	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8634	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8647	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8674	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine（脚本引擎）	CVE-2017-8646	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8659	Scripting Engine 信息泄露漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8671	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8672	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8639	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8640	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8637	Scripting Engine 安全功能绕过漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8670	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine（脚本引擎）	CVE-2017-8635	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8638	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine（脚本引擎）	CVE-2017-8636	Scripting Engine 内存破坏漏洞
Microsoft Windows	CVE-2017-0174	Windows NetBIOS 拒绝服务漏洞
Microsoft Windows	CVE-2017-8633	Windows 错误报告特权提升漏洞
Microsoft Windows PDF	CVE-2017-0293	Windows PDF 远程代码执行漏洞
Microsoft Windows Search Component（搜索组件）	CVE-2017-8620	Windows Search 远程代码执行漏洞

SQL Server	CVE-2017-8516	Microsoft SQL Server Analysis Services 信息泄露漏洞
Volume Manager Driver	CVE-2017-8668	Volume Manager Extension Driver 信息泄露漏洞
Windows Hyper-V	CVE-2017-8623	Windows Hyper-V 拒绝服务漏洞
Windows Hyper-V	CVE-2017-8664	Windows Hyper-V 远程代码执行漏洞
Windows Kernel-Mode Drivers（内核模式驱动）	CVE-2017-8666	Win32k 信息泄露漏洞
Windows Kernel-Mode Drivers（内核模式驱动）	CVE-2017-8691	Express Compressed Fonts 远程代码执行漏洞

Windows Kernel-Mode Drivers（内核模式驱动）	CVE-2017-8593	Win32k 特权提升漏洞
Windows RDP	CVE-2017-8673	Windows Remote Desktop Protocol (RDP) 拒绝服务漏洞
Windows Shell	CVE-2017-8591	Windows IME 远程代码执行漏洞
Windows Subsystem for Linux（适用于 Linux 的 Windows 子系统）	CVE-2017-8627	Windows Subsystem for Linux 拒绝服务漏洞
Windows Subsystem for Linux（适用于 Linux 的 Windows 子系统）	CVE-2017-8622	Windows Subsystem for Linux 特权提升漏洞

受影响的状况

见附件部分。

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

CVE-2017-8591 - Windows IME Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8591 MITRE NVD	**CVE Title:** Windows IME Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Windows Input Method Editor (IME) when IME improperly handles parameters in a method of a DCOM class. The DCOM server is a Windows component installed regardless of which languages/IMEs are enabled. An attacker can instantiate the DCOM class and exploit the system even if IME is not enabled. To exploit this vulnerability, a locally authenticated attacker could run a specially crafted application.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses this vulnerability by correcting how Windows IME handles parameters in a method of a DCOM class. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8591						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8591						
Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4034658 (Securit	Critical	Remote Code	4025339	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8591						
32-bit Systems	y Update)		Execution		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8591						
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8591						
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8591						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Critical	Remote Code Execution	4025331	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4034666 (Security Only) 4034665 (Monthl	Critical	Remote Code Execution	4025331	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8591						
	y Rollup)					
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4034672 (Security Only)	Critical	Remote Code	4025336	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8591						
Core installation)	4034681 (Monthly Rollup)		Execution		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4034658 (Securit	Critical	Remote Code Execution	4025339	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8591						
installation)	y Update)				CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	

CVE-2017-8593 - Win32k Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8593 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how Win32k handles objects in memory. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8593						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Elevation of Privilege	4025338	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Important	Elevation of Privilege	4025338	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Important	Elevation of Privilege	4025344	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4034660 (Security Update)	Important	Elevation of Privilege	4025344	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4034658 (Securit	Important	Elevation of	4025339	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8593						
32-bit Systems	y Update)		Privileg e		CVSS: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 1607 for x64-based Systems	403465 8 (Securit y Update)	Importan t	Elevatio n of Privileg e	4025339	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	403467 4 (Securit y Update)	Importan t	Elevatio n of Privileg e	4025342	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	Yes

CVE-2017-8593						
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Important	Elevation of Privilege	4025341	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
Windows 7 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4034672 (Security Only) 4034681 (Monthl	Important	Elevation of Privilege	4025336	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
	y Rollup)					
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthl	Important	Elevation of	4025336	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8593						
	y Rollup)		Privileg e		CVSS: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	403505 5 (Securit y Update)	Importan t	Elevatio n of Privileg e	4022887	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	Yes
Windows Server 2008 for 32-bit Systems Service	403505 5 (Securit y Update)	Importan t	Elevatio n of Privileg e	4022887	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	Yes

CVE-2017-8593						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4035055 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
Windows Server 2008 for x64-based Systems Service Pack 2	4035055 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4035055 (Security Update)	Important	Elevation of Privilege	4022887	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4034664 (Monthly	Important	Elevation of	4025341	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8593						
based Systems Service Pack 1	Rollup) 4034679 (Security Only)		Privilege		CVSS: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 R2 for x64-based Systems Service Pack 1 (Server Core	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
installation)						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Elevation of Privilege	4025331	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4034666 (Security Only)	Important	Elevation of	4025331	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8593						
Core installation)	4034665 (Monthly Rollup)		Privilege		CVSS: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 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8593						
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8634 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8634 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8634						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034674	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8634						
on Windows 10 Version 1703 for x64-based Systems	(Security 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	

CVE-2017-8635 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8635 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way JavaScript engines render when handling 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8635						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4034733 (IE Cumulative) 4034665 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025331	Base: 6.40 Temporal: 5.80 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 Window	4034668 (Security Update)	Critical	Remote Code	4025338	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8635						
s 10 for 32-bit Systems			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 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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 Window	4034660 (Security Update)	Critical	Remote Code	4025344	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8635						
s 10 Version 1511 for 32-bit Systems			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 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034733 (IE Cumulative) 4034681	Critical	Remote Code Execution	4025252 4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
32-bit systems	(Monthly Rollup)					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8635						
Windows RT 8.1					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2012 R2	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025336	Base: 6.40 Temporal: 5.80 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 Window	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 6.40 Temporal: 5.80 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-2017-8635						
s Server 2016						
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/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-	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Window	4034660 (Security Update)	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8635						
s 10 Version 1511 for x64-based Systems			Execution		CVSS: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	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
1703 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8635						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8636 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8636 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8636						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4034733 (IE Cumulative) 4034665 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025331	Base: 6.40 Temporal: 5.80 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 Window	4034668 (Security Update)	Critical	Remote Code	4025338	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8636						
s 10 for 32-bit Systems			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 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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 Window	4034660 (Security Update)	Critical	Remote Code	4025344	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8636						
s 10 Version 1511 for 32-bit Systems			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 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit	4034664 (Monthly Rollup) 4034733 (IE	Critical	Remote Code Execution	4025341 4025252	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Systems Service Pack 1	Cumulative)					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4034733 (IE Cumulative) 4034664 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025341	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Internet Explorer 11 on Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034733 (IE Cumulative) 4034664 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025341	Base: 6.40 Temporal: 5.80 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-2017-8636						
Internet Explorer 11 on Windows Server 2012 R2	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025336	Base: 6.40 Temporal: 5.80 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 Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 6.40 Temporal: 5.80 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-2017-8636						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 6.40 Temporal: 5.80 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	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 6.40 Temporal: 5.80 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-2017-8636						
x64-based Systems Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Microsoft Edge on Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8636						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8637 - Scripting Engine Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8637 MITRE NVD	**CVE Title:** Scripting Engine Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Edge as a result of how memory is accessed in code compiled by the Edge Just-In-Time (JIT) compiler that allows Arbitrary Code Guard (ACG) to be bypassed. By itself, this ACG bypass vulnerability does not allow arbitrary code execution. However, an	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	attacker could use the ACG 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 ACG bypass vulnerability, a user must be logged on and running an affected version of Microsoft Edge. The user would then need to browse to a malicious website. The security update addresses the ACG bypass vulnerability by helping to ensure that Microsoft Edge properly handles accessing memory in code compiled by the Edge JIT compiler. **FAQ:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8637						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Security Feature Bypass	4025342	Base: 3.70 Temporal: 3.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8637						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Security Feature Bypass	4025342	Base: 3.70 Temporal: 3.40 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8638 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8638 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 related 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. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8638						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8638						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8638						
x64-based Systems						

CVE-2017-8639 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8639 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8639						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034658	Critical	Remote Code	4025339	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8639						
on Windows 10 Version 1607 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8639						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034658 (Securit	Moderate	Remote Code	4025339	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8639						
Windows Server 2016	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8640 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8640 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8640						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Window	4034668 (Securit	Critical	Remote Code	4025338	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8640						
s 10 for x64-based Systems	y Update)		Execution		CVSS: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 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8640						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8640						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8640						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8640						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8662 - Microsoft Edge Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8662 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability for Microsoft Edge exists as a result of how strings are validated in specific scenarios, which can allow an attacker to read sensitive data from memory and thereby potentially bypass Address Space Layout Randomization (ASLR). By itself, this vulnerability does not allow arbitrary code execution. However, an attacker could use this vulnerability in conjunction with another vulnerability, such as a remote code execution vulnerability, to run arbitrary code on a target system. Successful exploitation of the vulnerability requires a user to be logged on and running an affected version of Microsoft Edge. The user would then need to browse to a malicious site. The security update addresses the vulnerability by helping to ensure that Microsoft Edge properly validates strings in affected scenarios. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8662						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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-2017-8662						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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-2017-8669 - Microsoft Browser Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8669 MITRE NVD	**CVE Title:** Microsoft Browser Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft browsers handle objects in memory while rendering content. 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	Moderate	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8669						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8669						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Internet Explorer 11 on Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/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	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025336	Base: 6.40 Temporal: 5.80 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-2017-8669						
Internet Explorer 11 on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Microsoft Edge on Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8669						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8670 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8670 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8670						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034658	Critical	Remote Code	4025339	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8670						
on Windows 10 Version 1607 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8670						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034658 (Securit	Moderate	Remote Code	4025339	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8670						
Windows Server 2016	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8671 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8671 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8671						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8671						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8671						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8671						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8671						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8672 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8672 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8672						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Window	4034668 (Securit	Critical	Remote Code	4025338	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8672						
s 10 for x64-based Systems	y Update)		Execution		CVSS: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 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8672						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8672						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8672						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8672						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8654 - Microsoft Office SharePoint XSS Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8654 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8654						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8654						
Microsoft SharePoint Server 2010 Service Pack 2	2956077 (Security Update)	Important	Spoofing	2837598	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-0174 - Windows NetBIOS Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-0174 MITRE NVD	**CVE Title:** Windows NetBIOS Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Windows improperly handles NetBIOS packets. An attacker who successfully exploited this vulnerability could cause a target computer to become completely unresponsive. A remote unauthenticated attacker could exploit this vulnerability by sending a series of TCP packets to a target system, resulting in a permanent denial of service condition. The update addresses the vulnerability by correcting how the Windows network stack handles NetBIOS traffic. **FAQ:** None **Mitigations:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-0174						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-0174						
Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Denial of Service	4025338	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Important	Denial of Service	4025338	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4034660 (Securit	Important	Denial of	4025344	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-0174						
32-bit Systems	y Update)		Service		CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Denial of Service	4025344	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Important	Denial of Service	4025339	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Denial of Service	4025339	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Denial of Service	4025342	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4034674 (Securit	Important	Denial of	4025342	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-0174						
x64-based Systems	y Update)		Service		CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Important	Denial of Service	4025341	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4034664 (Monthly	Important	Denial of	4025341	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-0174						
Service Pack 1	Rollup) 4034679 (Security Only)		Service		CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Denial of Service	4025336	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Denial of Service	4025336	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthly Rollup)	Important	Denial of Service	4025336	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
Windows Server 2008 for 32-bit Systems Service Pack 2	4022750 (Security Update)	Important	Denial of Service	4021923	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core	4022750 (Security Update)	Important	Denial of Service	4021923	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4022750 (Security Update)	Important	Denial of Service	4021923	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4022750 (Securit	Important	Denial of Service	4021923	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-0174						
Service Pack 2	y Update)				CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4022750 (Security Update)	Important	Denial of Service	4021923	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Denial of Service	4025341	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4034664 (Monthly Rollup) 4034679	Important	Denial of Service	4025341	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
Service Pack 1	(Security Only)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Denial of Service	4025341	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Denial of Service	4025331	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4034666 (Security Only) 4034665 (Monthl	Important	Denial of Service	4025331	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0174						
	y Rollup)					
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Denial of Service	4025336	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4034672 (Security Only)	Important	Denial of	4025336	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-0174						
Core installation)	4034681 (Monthly Rollup)		Service		CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4034658 (Security Update)	Important	Denial of Service	4025339	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4034658 (Securit	Important	Denial of Service	4025339	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-0174						
installation)	y Update)				CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	

CVE-2017-0250 - Microsoft JET Database Engine Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-0250 MITRE NVD	**CVE Title:** Microsoft JET Database Engine Remote Code Execution Vulnerability **Description:** A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of this vulnerability requires that a user open or preview a specially crafted database file while using an affected version of Microsoft Windows. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted database file to the user and then convincing the user to open the file. The update addresses the vulnerability by modifying how the Microsoft JET Database Engine handles objects in memory.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** **Workarounds:** • **Restrict the Microsoft Jet Database Engine from running for any application** To implement the workaround, enter the following command at a command prompt: `echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /P everyone:N` **Impact of workaround.** Any application requiring the use of the Microsoft Jet Database Engine to make data access calls will not function. **How to undo the workaround.** Enter the following command at a command		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	prompt echo y| cacls "%SystemRoot%\system32\msjet40.dll" /E /R everyone • **Use group policy to restrict the Microsoft Jet Database Engine from running for any application** To implement the workaround, perform the following steps: 1. Create the following script, named JetCacls.cmd for illustration: @echo off if exist %systemdrive%\Cacls.log goto end cacls "%SystemRoot%\system32\msjet40.dll" /E /P everyone:N > nul 2>&1 echo %date% %time%: Msjet Cacls updated > %systemdrive%\Cacls.log :end exit 2. Copy JetCacls.cmd to the Netlogon shared folder, or another shared folder on the domain controller from which JetCacls.cmd would run.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. Set up JetCacls.cmd. In the **Active Directory Users and Computers MMC** snap-in, right-click the domain name, and then click **Properties**. 4. Click the **Group Policy** tab. 5. Click **New** to create a new Group Policy object (GPO), and enter JetCacls for the name of the policy. 6. Click the new policy, and then click **Edit**. 7. Expand **Windows Settings for Computer Configuration**, and then click **Scripts**. 8. Double-click **Logon**, and then click **Add**. The Add a Script dialog box appears. 9. Type *servername**sharename*\JetCacls.cmd in the Script Name box. 10. Click **OK**, and then click **Apply**. 11. Then restart the client computers that are members of this domain. **Impact of workaround.** Any application that requires the use of the Microsoft Jet Database Engine to make data access calls will not function. This restriction only applies to applications that are running on client computers in the domain.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-0250						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-0250						
Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4034660 (Securit	Critical	Remote Code	4025344	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-0250						
32-bit Systems	y Update)		Execution		CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4034674 (Securit	Critical	Remote Code	4025342	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-0250						
x64-based Systems	y Update)		Execution		CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Critical	Remote Code Execution	4025341	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4034664 (Monthly	Critical	Remote Code	4025341	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-0250						
Service Pack 1	Rollup) 4034679 (Security Only)		Execution		CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
Windows Server 2008 for 32-bit Systems Service Pack 2	4034775 (Security Update)	Critical	Remote Code Execution	None	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core	4034775 (Security Update)	Critical	Remote Code Execution	None	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4034775 (Security Update)	Critical	Remote Code Execution	None	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4034775 (Securit	Critical	Remote Code Execution	None	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-0250						
Service Pack 2	y Update)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4034775 (Security Update)	Critical	Remote Code Execution	None	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server	4034664	Critical	Remote Code	4025341	Base: 7.80 Temporal: 7.00	Yes

CVE-2017-0250						
2008 R2 for Itanium-Based Systems Service Pack 1	(Monthly Rollup) 4034679 (Security Only)		Execution		Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Critical	Remote Code Execution	4025341	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4034664 (Monthly Rollup) 4034679 (Security Only)	Critical	Remote Code Execution	4025341	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4034666 (Security Only)	Critical	Remote Code Execution	4025331	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-0250						
	4034665 (Monthly Rollup)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4034666 (Security Only) 4034665 (Monthly Rollup)	Critical	Remote Code Execution	4025331	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthl	Critical	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0250						
	y Rollup)					
Windows Server 2016	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-0293 - Windows PDF Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-0293 MITRE NVD	**CVE Title:** Windows PDF Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit the vulnerability on Windows 10 systems with Microsoft Edge set as the default browser, an attacker could host a specially crafted website that contains malicious PDF content and then convince users to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted PDF content to such sites. Only Windows 10 systems with Microsoft Edge set as the default browser can be compromised simply by viewing a website. The browsers for all other affected operating systems do not automatically render PDF content, so an attacker would have no way to force users to view attacker-controlled content. Instead, an attacker would have to convince users to open a specially crafted PDF document, typically by way of an enticement in an email or instant message or by way of an email attachment. The update addresses the vulnerability by modifying how affected systems handle objects in memory.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-0293						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4034658 (Securit	Critical	Remote Code	4025339	Base: 3.60 Temporal: 3.30 Vector:	Yes

CVE-2017-0293						
32-bit Systems	y Update)		Execution		CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Critical	Remote Code Execution	4025341	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4034664 (Monthly Rollup) 4034679	Critical	Remote Code Execution	4025341	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
Service Pack 1	(Security Only)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4034664 (Monthly Rollup) 4034679 (Security Only)	Critical	Remote Code Execution	4025341	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Critical	Remote Code Execution	4025331	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4034666 (Security Only) 4034665 (Monthl	Critical	Remote Code Execution	4025331	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0293						
	y Rollup)					
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4034672 (Security Only)	Critical	Remote Code	4025336	Base: 3.60 Temporal: 3.30 Vector:	Yes

CVE-2017-0293						
Core installation)	4034681 (Monthly Rollup)		Execution		CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Windows Server 2016	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 3.60 Temporal: 3.30 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4034658 (Securit	Critical	Remote Code Execution	4025339	Base: 3.60 Temporal: 3.30 Vector:	Yes

CVE-2017-0293						
installation)	y Update)				CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8503 - Microsoft Edge Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8503 MITRE NVD	**CVE Title:** Microsoft Edge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser. An attacker who successfully exploited this vulnerability could gain elevated privileges and break out of the Edge AppContainer sandbox. The vulnerability by itself does not allow arbitrary code to run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (for example a remote code execution vulnerability and another elevation of privilege vulnerability) to take advantage of the elevated privileges when running.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Microsoft Edge handles sandboxing. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8503						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Important	Elevation of Privilege	4025344	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8503						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Elevation of Privilege	4025344	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8503						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8503						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8503						
x64-based Systems						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Low	Elevation of Privilege	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8516 - Microsoft SQL Server Analysis Services Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8516 MITRE NVD	**CVE Title:** Microsoft SQL Server Analysis Services Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft SQL Server Analysis Services when it improperly enforces permissions. An attacker could exploit the vulnerability if the attacker's credentials allow access to an affected SQL server database. An attacker who successfully exploited the vulnerability could gain additional database and file information. The security update addresses the vulnerability by correcting how SQL Server Analysis Services	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	enforces permissions. **FAQ:** **There are GDR and/or CU (Cumulative Update) updates offered for my version of SQL Server. How do I know which update to use?** First, determine your SQL Server version number. For more information on determining your SQL Server version number, see Microsoft Knowledge Base Article TBD. Second, in the table below, locate your version number or the version range that your version number falls within. The corresponding update is the one you need to install. **Note** If your SQL Server version number is not represented in the table below, your SQL Server version is no longer supported. Please upgrade to the latest Service Pack or SQL Server product in order to apply this and future security updates. **Update number** / **Title** / **Apply if current product version is...** / **This securit also inc servicing re throug**		

CVE ID	Vulnerability Description				Maximum Severity Rating	Vulnerability Impact
	4019092	Description of the security update for SQL Server 2012 SP3 GDR: August 8, 2017	11.0.6020.0 - 11.0.6248.0	3194721		
	4019090	Description of the security update for SQL Server 2012 SP3 CU: August 8, 2017	11.0.6518.0 - 11.0.6598.0	3194724		
	4019091	Description of the security update for SQL Server 2014 Service Pack 1 GDR: August 8, 2017	12.0.4100.1 - 12.0.4232.0	3194720		
	4032542	Description of the security update for SQL Server 2014 Service Pack 1 CU: August 8, 2017	12.0.4416.0 - 12.0.4511.0	3194720		
	4019093	Description of the security update for SQL Server 2014 Service Pack 2 GDR: August 8, 2017	12.0.5000.0 - 12.0.5203.0	3194714		
	4036996	Description of the security update for SQL Server 2014 Service Pack 2 CU: August 8, 2017	12.0.5511.0 - 12.0.5546.0	3194718		
	4019088	Description of the security update for SQL Server 2016 RTM GDR: August 8, 2017	13.0.1601.5 - 13.0.1722.0	3194716		
	4019086	Description of the security update for SQL Server 2016 RTM CU: August 8, 2017	13.0.2149.0 - 13.0.2204.0	3194717		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

4019089	Description of the security update for SQL Server 2016 Service Pack 1 GDR: August 8, 2017	13.0.1605.0 - 13.0.1721.0	Not applicable
4019095	Description of the security update for SQL Server 2016 CU: November 8, 2016	13.0.4411.0 - 13.0.4435.0	Not applicable

For additional installation instructions, see the Security Update Information subsection for your SQL Server edition in the **Update Information** section.

What are the GDR and CU update designations and how do they differ?
The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different update servicing branches in place for SQL Server. The primary difference between the two is that CU branches cumulatively include *all* updates for a given baseline, while GDR branches include *only* cumulative critical updates for a given baseline. A baseline can be the initial RTM release or a Service Pack.

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	For any given baseline, either the GDR or CU branch updates are options if you are at the baseline or have only installed a previous GDR update for that baseline. The CU branch is the only option if you have installed a previous SQL Server CU for the baseline you are on. **Will these security updates be offered to SQL Server clusters?** Yes. The updates will also be offered to SQL Server 2012 SP2/SP3, SQL Server 2014 SP1/SP2, SQL Server 2016 RTM and SQL Server 2016 SP1 instances that are clustered. Updates for SQL Server clusters will require user interaction. If the SQL Server 2012 SP2/SP3, SQL Server 2014 SP1/SP2, SQL Server 2016 RTM and SQL Server 2016 SP1 cluster has a passive node, to reduce downtime, Microsoft recommends that you scan and apply the update to the inactive node first, then scan and apply it to the active node. When all components have been updated on all nodes, the update will no longer be offered. **Can the security updates be applied to SQL Server instances on Windows Azure (IaaS)?** Yes. SQL Server instances on Windows Azure (IaaS) can be offered the security updates through Microsoft Update, or customers can download the security updates from Microsoft Download Center and apply them manually.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8516						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SQL Server 2012 for 32-bit Systems Service Pack 3	4019092 (Security Update)	Important	Information Disclosure	3194721	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2012 for 32-bit Systems Service Pack 3 (CU)	4019090 (Security Update)	Important	Information Disclosure	3194724	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8516						
Microsoft SQL Server 2012 for x64-based Systems Service Pack 3	4019092 (Security Update)	Important	Information Disclosure	3194721	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2012 for x64-based Systems Service Pack 3 (CU)	4019090 (Security Update)	Important	Information Disclosure	3194724	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 1 for 32-bit Systems	4019091 (Security Update)	Important	Information Disclosure	3194720	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8516						
Microsoft SQL Server 2014 Service Pack 1 for 32-bit Systems (CU)	4032542 (Security Update)	Important	Information Disclosure	3194720	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 1 for x64-based Systems	4019091 (Security Update)	Important	Information Disclosure	3194720	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 1 for x64-based Systems (CU)	4032542 (Security Update)	Important	Information Disclosure	3194720	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8516						
Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems	4019093 (Security Update)	Important	Information Disclosure	3194714	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (CU)	4036996 (Security Update)	Important	Information Disclosure	3194718	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems	4019093 (Security Update)	Important	Information Disclosure	3194714	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8516						
Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (CU)	4036996 (Security Update)	Important	Information Disclosure	3194718	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems	4019088 (Security Update)	Important	Information Disclosure	3194716	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems (CU)	4019086 (Security Update)	Important	Information Disclosure	3194717	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8516						
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1	4019089 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU)	4019095 (Security Update)	Important	Information Disclosure	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8620 - Windows Search Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8620 MITRE NVD	**CVE Title:** Windows Search Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Search handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. An attacker with access to a target computer could exploit this vulnerability to elevate privileges and take control of the computer. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger the vulnerability through an SMB connection and then take control of a target computer. The security update addresses the vulnerability by correcting how Windows Search handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Disable WSearch service Interactive workaround deployment steps 1. Click **Start**, click **Run**, type "regedit" (without the quotation marks), and then click **OK**. 2. Expand HKEY_LOCAL_MACHINE 3. Expand System, then CurrentControlSet, then Services 4. Click on **WSearch** 5. Click the **File** menu and select Export. 6. In the **Export Registry File** dialog type "WSearch_configuration_backup.reg" and press **Save**. 7. Double-click the value named **Start** and change the **Value** data field to 4 8. Click **OK** 9. Run the following command at a command prompt running as an administrator: **sc stop WSearch**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How do undo the workaround 1. Click **Start** , click **Run** , type "regedit " (without the quotation marks), and then click **OK**. 2. Click the **File** menu and select Import. 3. In the **Import Registry File** dialog select "WSearch_configuration_backup.reg" and press **Open**. Managed workaround deployment steps 1. First a backup copy of the registry keys can be made from a managed deployment script with the following command: **regedit /e WSearch_configuration_backup.reg HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2. Next save the following to a file with a .REG extension (e.g. Disable_WSearch.reg) **Windows Registry Editor Version 5.00** **[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch]** **"Start"=dword:00000004** 3. Run the registry script created in step 2 on the target machine with the following command: **regedit /s Disable_WSearch .reg** 4. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How to undo the workaround Restore the original state by running the following command: **regedit /s WSearch_configuration_backup.reg**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8620						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8620						
Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4034660 (Securit	Critical	Remote Code	4025344	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8620						
32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4034674 (Securit	Critical	Remote Code	4025342	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8620						
x64-based Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Critical	Remote Code Execution	4025341	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4034664 (Monthly	Critical	Remote Code	4025341	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8620						
Service Pack 1	Rollup) 4034679 (Security Only)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
Windows Server 2008 for 32-bit Systems Service Pack 2	4034034 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core	4034034 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4034034 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4034034 (Securit	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8620						
Service Pack 2	y Update)				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4034034 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server	4034664	Critical	Remote Code	4025341	Base: 8.10 Temporal: 7.30	Yes

CVE-2017-8620						
2008 R2 for Itanium-Based Systems Service Pack 1	(Monthly Rollup) 4034679 (Security Only)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Critical	Remote Code Execution	4025341	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4034664 (Monthly Rollup) 4034679 (Security Only)	Critical	Remote Code Execution	4025341	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4034666 (Security Only)	Critical	Remote Code Execution	4025331	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8620						
	4034665 (Monthly Rollup)				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4034666 (Security Only) 4034665 (Monthly Rollup)	Critical	Remote Code Execution	4025331	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthl	Critical	Remote Code Execution	4025336	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8620						
	y Rollup)					
Windows Server 2016	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8622 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8622 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles NT pipes. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.	Critical	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 NT pipes. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8622						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8622						
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Elevation of Privilege	4025342	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8623 - Windows Hyper-V Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8623 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8623						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8623						
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Denial of Service	4025339	Base: 5.80 Temporal: 5.20 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Denial of Service	4025342	Base: 5.80 Temporal: 5.20 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8623						
Windows Server 2016	4034658 (Security Update)	Important	Denial of Service	4025339	Base: 5.80 Temporal: 5.20 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Important	Denial of Service	4025339	Base: 5.80 Temporal: 5.20 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624 - Windows CLFS Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8624 MITRE NVD	**CVE Title:** Windows CLFS Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	control of the affected system. An attacker who successfully exploited this vulnerability could run processes in an elevated context. The update addresses the vulnerability by correcting how CLFS handles objects in memory. Note: The Common Log File System (CLFS) is a high-performance, general-purpose log file subsystem that dedicated client applications can use and multiple clients can share to optimize log access. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8624						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Elevation of Privilege	4025338	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for	4034668 (Securit	Important	Elevation of	4025338	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8624						
x64-based Systems	y Update)		Privileg e		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/ RC:C	
Windows 10 Version 1511 for 32-bit Systems	403466 0 (Securit y Update)	Importan t	Elevatio n of Privileg e	4025344	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/ RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	403466 0 (Securit y Update)	Importan t	Elevatio n of Privileg e	4025344	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/ RC:C	Yes

CVE-2017-8624						
Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4034674 (Securit	Important	Elevation of	4025342	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8624						
32-bit Systems	y Update)		Privilege		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthl	Important	Elevation of Privilege	4025341	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
	y Rollup)					
Windows 7 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-	4034672 (Security Only)	Important	Elevation of	4025336	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8624						
bit systems	4034681 (Monthly Rollup)		Privilege		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
Windows RT 8.1	4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4034745 (Security Update)	Important	Elevation of Privilege	3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4034745 (Security Update)	Important	Elevation of Privilege	3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based	4034745 (Security Update)	Important	Elevation of Privilege	3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
Systems Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4034745 (Security Update)	Important	Elevation of Privilege	3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4034745 (Securit	Important	Elevation of Privilege	3203838	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8624						
Service Pack 2 (Server Core installation)	y Update)				CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service	4034664 (Monthly Rollup) 4034679	Important	Elevation of Privilege	4025341	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
Pack 1 (Server Core installation)	(Security Only)					
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Elevation of Privilege	4025331	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
Windows Server 2012 (Server Core installation)	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Elevation of Privilege	4025331	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthl	Important	Elevation of Privilege	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8624						
	y Rollup)					
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4034658 (Securit	Important	Elevation of	4025339	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8624						
	y Update)		Privilege		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8625 - Internet Explorer Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8625 MITRE NVD	**CVE Title:** Internet Explorer Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Internet Explorer fails to validate User Mode Code Integrity (UMCI) policies. The vulnerability could allow an attacker to bypass Device Guard UCMI policies. To exploit the vulnerability, a user could either visit a malicious website or an attacker with access to the system could run a specially crafted application. An	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	attacker could then leverage the vulnerability to run unsigned malicious code as though it were signed by a trusted source. The update addresses the vulnerability by correcting how Internet Explorer validates UMCI policies. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8625						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Security Feature Bypass	4025338	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Window	4034668 (Securit	Important	Security	4025338	Base: 5.30 Temporal: 4.80 Vector:	Yes

CVE-2017-8625						
s 10 for x64-based Systems	y Update)		Feature Bypass		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Important	Security Feature Bypass	4025344	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8625						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Security Feature Bypass	4025344	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4034658 (Security Update)	Important	Security Feature Bypass	4025339	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8625						
1607 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Security Feature Bypass	4025339	Base: 5.30 Temporal: 4.80 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Internet Explorer	4034658	Low	Security	4025339	Base: 5.30 Temporal: 4.80	Yes

CVE-2017-8625						
11 on Windows Server 2016	(Security Update)		Feature Bypass		Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	

CVE-2017-8627 - Windows Subsystem for Linux Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8627 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory. An attacker who successfully exploited this vulnerability could cause a denial of service against the local system. A attacker could exploit this vulnerability by running a specially crafted application. The update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8627						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Denial of Service	4025342	Base: 4.40 Temporal: 4.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633 - Windows Error Reporting Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8633 MITRE NVD	**CVE Title:** Windows Error Reporting Elevation of Privilege Vulnerability **Description:** This security update resolves a vulnerability in Windows Error Reporting (WER). The vulnerability could allow elevation of privilege if successfully exploited by an attacker. An attacker who successfully exploited this vulnerability could gain greater access to sensitive information and system functionality. To exploit this vulnerability, an attacker would run a specially crafted application. This update corrects the way the WER handles and executes files. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8633						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Elevation of Privilege	4025338	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Important	Elevation of Privilege	4025338	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Important	Elevation of Privilege	4025344	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/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	4034660 (Security Update)	Important	Elevation of Privilege	4025344	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/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	4034658 (Securit	Important	Elevation of	4025339	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8633						
32-bit Systems	y Update)		Privileg e		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	
Windows 10 Version 1607 for x64-based Systems	403465 8 (Securit y Update)	Importa nt	Elevatio n of Privileg e	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/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	403467 4 (Securit y Update)	Importa nt	Elevatio n of Privileg e	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	Yes

CVE-2017-8633						
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Important	Elevation of Privilege	4025341	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
Windows 7 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/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	4034672 (Security Only) 4034681 (Monthl	Important	Elevation of Privilege	4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
	y Rollup)					
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthl	Important	Elevation of	4025336	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8633						
	y Rollup)		Privileg e		CVSS:3.0/AV:N/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	403567 9 (Securit y Update)	Importa nt	Elevatio n of Privileg e	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	Yes
Windows Server 2008 for 32-bit Systems Service	403567 9 (Securit y Update)	Importa nt	Elevatio n of Privileg e	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O /RC:C	Yes

CVE-2017-8633						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4035679 (Security Update)	Important	Elevation of Privilege	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
Windows Server 2008 for x64-based Systems Service Pack 2	4035679 (Security Update)	Important	Elevation of Privilege	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/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	4035679 (Security Update)	Important	Elevation of Privilege	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4034664 (Monthly	Important	Elevation of	4025341	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8633						
based Systems Service Pack 1	Rollup) 4034679 (Security Only)		Privilege		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Elevation of Privilege	4025341	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
installation)						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Elevation of Privilege	4025331	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/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	4034666 (Security Only)	Important	Elevation of	4025331	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8633						
Core installation)	4034665 (Monthly Rollup)		Privilege		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Elevation of Privilege	4025336	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8633						
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Important	Elevation of Privilege	4025339	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8641 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8641 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way JavaScript engines render when handling 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8641						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4034733 (IE Cumulative) 4034665 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025331	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Window	4034668 (Security Update)	Critical	Remote Code	4025338	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8641						
s 10 for 32-bit Systems			Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Window	4034660 (Security Update)	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8641						
s 10 Version 1511 for 32-bit Systems			Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit	4034664 (Monthly Rollup) 4034733 (IE	Critical	Remote Code Execution	4025341 4025252	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Systems Service Pack 1	Cumulative)					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4034733 (IE Cumulative) 4034664 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025341	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Internet Explorer 11 on Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034733 (IE Cumulative) 4034664 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025341	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Internet Explorer 11 on Windows Server 2012 R2	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025336	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
x64-based Systems Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Microsoft Edge on Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8641						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8642 - Microsoft Edge Elevation of Privilege Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8642 MITRE NVD	**CVE Title:** Microsoft Edge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Edge does not properly validate JavaScript under specific conditions, potentially allowing script to run with elevated privileges.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. An attacker who successfully exploited the vulnerability could elevate privileges in affected versions of Microsoft Edge. An attacker could then leverage these privileges with another vulnerability to run arbitrary code with medium integrity level privileges (permissions of the current user).		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Edge validates and sanitizes JavaScript parameters. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8642						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 6.10 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8642						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Elevation of Privilege	4025342	Base: 6.10 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8644 - Microsoft Edge Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8644 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 certain functions handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8644						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Information Disclosure	4025338	Base: 4.30 Temporal: 3.90 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-2017-8644						
Microsoft Edge on Windows 10 for x64-based Systems	4034668 (Security Update)	Important	Information Disclosure	4025338	Base: 4.30 Temporal: 3.90 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	4034660 (Security Update)	Important	Information Disclosure	4025344	Base: 4.30 Temporal: 3.90 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-2017-8644						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Information Disclosure	4025344	Base: 4.30 Temporal: 3.90 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-2017-8644						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 4.30 Temporal: 3.90 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	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 4.30 Temporal: 3.90 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-2017-8644						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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-2017-8644						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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	4034658 (Security Update)	Low	Information Disclosure	4025339	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8645 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8645 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8645						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8645						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8645						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8645						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8645						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8646 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8646 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8646						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8646						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8646						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8646						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8646						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8647 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8647 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8647						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034674	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8647						
on Windows 10 Version 1703 for x64-based Systems	(Security 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	

CVE-2017-8650 - Microsoft Edge Security Feature Bypass Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8650 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft Edge does not properly enforce same-origin policies, which could allow an attacker to access information from origins outside the current one. In a web-based attack scenario, an attacker could trick a user into loading a webpage with malicious content. To exploit the vulnerability, an attacker would need to trick a user into loading a page or visiting a website. The webpage could also be injected into a compromised site or ad network. The security update addresses the vulnerability by helping to ensure that cross-domain policies are properly enforced in Microsoft Edge. **FAQ:** None **Mitigations:**	Moderate	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8650						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8650						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Moderate	Security Feature Bypass	4025342	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR: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	4034674 (Security Update)	Moderate	Security Feature Bypass	4025342	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8650						
x64-based Systems						

CVE-2017-8651 - Internet Explorer Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8651 MITRE NVD	**CVE Title:** Internet Explorer Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force users to view the attacker-	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	controlled content. Instead, an attacker would have to convince users to take action, typically by an enticement in an email or instant message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8651						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 10 on Windows Server 2012	4034733 (IE Cumulative) 4034665 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025331	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Window	4034733 (IE	Moderate	Remote Code	4025252	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8651						
s Server 2008 for 32-bit Systems Service Pack 2	Cumulative)		Execution			
Internet Explorer 9 on Windows Server 2008 for x64-based Systems	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8651						
Service Pack 2						

CVE-2017-8652 - Microsoft Edge Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8652 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how certain functions handle objects in memory.	Low	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8652						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Information Disclosure	4025338	Base: 4.30 Temporal: 3.90 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 Window	4034668 (Security	Important	Information Disclosure	4025338	Base: 4.30 Temporal: 3.90 Vector:	Yes

CVE-2017-8652						
s 10 for x64-based 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 1511 for 32-bit Systems	4034660 (Security Update)	Important	Information Disclosure	4025344	Base: 4.30 Temporal: 3.90 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-2017-8652						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Information Disclosure	4025344	Base: 4.30 Temporal: 3.90 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	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 4.30 Temporal: 3.90 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-2017-8652						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 4.30 Temporal: 3.90 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-2017-8652						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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-2017-8652						
x64-based Systems						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Low	Information Disclosure	4025339	Base: 2.40 Temporal: 2.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653 - Microsoft Browser Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8653 MITRE NVD	**CVE Title:** Microsoft Browser Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft browsers improperly access objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8653						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8653						
Internet Explorer 10 on Windows Server 2012	4034733 (IE Cumulative) 4034665 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025331	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 11 on Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit	4034664 (Monthly Rollup) 4034733 (IE	Critical	Remote Code Execution	4025341 4025252	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Systems Service Pack 1	Cumulative)					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4034733 (IE Cumulative) 4034664 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025341	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025252 4025336	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 11 on Windows RT 8.1	4034681 (Monthly Rollup)	Critical	Remote Code Execution	4025336	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034733 (IE Cumulative) 4034664 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025341	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 11 on Windows Server 2012 R2	4034733 (IE Cumulative) 4034681 (Monthly Rollup)	Moderate	Remote Code Execution	4025252 4025336	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for	4034733 (IE Cumulative)	Moderate	Remote Code Execution	4025252	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
x64-based Systems Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Microsoft Edge on Windows 10 for x64-based Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8653						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8655 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8655 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8655						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4034668 (Security Update)	Critical	Remote Code Execution	4025338	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Window	4034668 (Securit	Critical	Remote Code	4025338	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8655						
s 10 for x64-based Systems	y Update)		Execution		CVSS: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 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8655						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8655						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8655						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8655						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8656 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8656 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8656						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034658	Critical	Remote Code	4025339	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8656						
on Windows 10 Version 1607 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8656						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034658 (Securit	Moderate	Remote Code	4025339	Base: 3.10 Temporal: 2.80 Vector:	Yes

CVE-2017-8656						
Windows Server 2016	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8657 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8657 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8657						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4034660 (Security Update)	Critical	Remote Code Execution	4025344	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034660	Critical	Remote Code	4025344	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8657						
on Windows 10 Version 1511 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8657						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034674 (Securit	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8657						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8657						
Microsoft Edge on Windows Server 2016	4034658 (Security Update)	Moderate	Remote Code Execution	4025339	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8659 - Scripting Engine Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8659 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Chakra scripting engine does not properly handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user'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 certain functions handle objects in memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8659						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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-2017-8659						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 4.30 Temporal: 3.90 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-2017-8661 - Microsoft Edge Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8661 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 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 scripting 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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how affected Microsoft scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8661						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Critical	Remote Code Execution	4025339	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034658	Critical	Remote Code	4025339	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8661						
on Windows 10 Version 1607 for x64-based Systems	(Security Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8661						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4034658 (Securit	Moderate	Remote Code	4025339	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8661						
Windows Server 2016	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8664 - Windows Hyper-V Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8664 MITRE NVD	**CVE Title:** Windows Hyper-V Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code. An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8664						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8664						
Windows 10 for x64-based Systems	4034668 (Security Update)	Important	Remote Code Execution	4025338	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Remote Code Execution	4025344	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4034658 (Securit	Important	Remote Code	4025339	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-8664						
x64-based Systems	y Update)		Execution		CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Remote Code Execution	4025342	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthl	Important	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8664						
	y Rollup)					
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Remote Code Execution	4025331	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4034666 (Security Only)	Important	Remote Code	4025331	Base: 7.80 Temporal: 7.00 Vector:	Yes

CVE-2017-8664						
Core installation)	4034665 (Monthly Rollup)		Execution		CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8664						
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Remote Code Execution	4025336	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4034658 (Security Update)	Important	Remote Code Execution	4025339	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8664						
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Important	Remote Code Execution	4025339	Base: 7.80 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8666 - Win32k Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8666 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the win32k component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how win32k handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8666						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8666						
Windows 10 for 32-bit Systems	4034668 (Security Update)	Important	Information Disclosure	4025338	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4034668 (Security Update)	Important	Information Disclosure	4025338	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4034660 (Securit	Important	Information Disclosure	4025344	Base: 7.00 Temporal: 6.50 Vector:	Yes

CVE-2017-8666						
32-bit Systems	y Update)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	
Windows 10 Version 1511 for x64-based Systems	4034660 (Security Update)	Important	Information Disclosure	4025344	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Windows 10 Version 1607 for x64-based Systems	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Windows 10 Version 1703 for x64-based Systems	4034674 (Security Update)	Important	Information Disclosure	4025342	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Important	Information Disclosure	4025341	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Windows 7 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Information Disclosure	4025341	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthl	Important	Information Disclosure	4025336	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
	y Rollup)					
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Information Disclosure	4025336	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthl	Important	Information Disclosure	4025336	Base: 7.00 Temporal: 6.50 Vector:	Yes

CVE-2017-8666						
	y Rollup)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4035055 (Security Update)	Important	Information Disclosure	4022887	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service	4035055 (Security Update)	Important	Information Disclosure	4022887	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4035055 (Security Update)	Important	Information Disclosure	4022887	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Windows Server 2008 for x64-based Systems Service Pack 2	4035055 (Security Update)	Important	Information Disclosure	4022887	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core	4035055 (Security Update)	Important	Information Disclosure	4022887	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Information Disclosure	4025341	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4034664 (Monthly	Important	Information Disclosure	4025341	Base: 7.00 Temporal: 6.50 Vector:	Yes

CVE-2017-8666						
based Systems Service Pack 1	Rollup) 4034679 (Security Only)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Information Disclosure	4025341	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
installation)						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Information Disclosure	4025331	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server	4034666 (Security Only)	Important	Information Disclosure	4025331	Base: 7.00 Temporal: 6.50 Vector:	Yes

CVE-2017-8666						
Core installation)	4034665 (Monthly Rollup)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Information Disclosure	4025336	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Information Disclosure	4025336	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2016	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8666						
Windows Server 2016 (Server Core installation)	4034658 (Security Update)	Important	Information Disclosure	4025339	Base: 7.00 Temporal: 6.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8668 - Volume Manager Extension Driver Information Disclosure Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8668 MITRE NVD	**CVE Title:** Volume Manager Extension Driver Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Volume Manager Extension Driver component improperly provides kernel information. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Volume Manager Extension Driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8668						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Important	Information Disclosure	4025341	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2017-8668						
Windows 7 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Information Disclosure	4025341	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4034672 (Security Only) 4034681 (Monthl	Important	Information Disclosure	4025336	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2017-8668						
	y Rollup)					
Windows 8.1 for x64-based systems	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Information Disclosure	4025336	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows RT 8.1	4034681 (Monthl	Important	Information Disclosure	4025336	Base: 4.70 Temporal: 4.10 Vector:	Yes

CVE-2017-8668						
	y Rollup)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4034744 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service	4034744 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2017-8668						
Pack 2 (Server Core installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4034744 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes

CVE-2017-8668						
Windows Server 2008 for x64-based Systems Service Pack 2	4034744 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core	4034744 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	Yes

CVE-2017-8668						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Information Disclosure	4025341	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	Yes
Windows Server 2008 R2 for x64-	4034664 (Monthly	Important	Information Disclosure	4025341	Base: 4.70 Temporal: 4.10 Vector:	Yes

CVE-2017-8668						
based Systems Service Pack 1	Rollup) 4034679 (Security Only)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Information Disclosure	4025341	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	Yes

CVE-2017-8668						
installation)						
Windows Server 2012	4034666 (Security Only) 4034665 (Monthly Rollup)	Important	Information Disclosure	4025331	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	Yes
Windows Server 2012 (Server	4034666 (Security Only)	Important	Information Disclosure	4025331	Base: 4.70 Temporal: 4.10 Vector:	Yes

CVE-2017-8668						
Core installation)	4034665 (Monthly Rollup)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	
Windows Server 2012 R2	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Information Disclosure	4025336	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	Yes

CVE-2017-8668						
Windows Server 2012 R2 (Server Core installation)	4034672 (Security Only) 4034681 (Monthly Rollup)	Important	Information Disclosure	4025336	Base: 4.70 Temporal: 4.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O	Yes

ADV170010 - August 2017 Flash Update

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170010 MITRE NVD	**CVE Title:** August 2017 Flash Update **Description:** This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin APSB17-23: CVE-2017-3085, CVE-2017-3106 **FAQ:** **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: **Workarounds:** Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update. • **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. Paste the following into a text file and save it with the .reg file extension. Copy Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround. • **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy** **Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites: Group Policy Overview		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What is Group Policy Object Editor? Core Group Policy tools and settings To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010. 1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates** -> **Windows Components** -> **Internet Explorer** -> **Security Features** -> **Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	4. Change the setting to **Enabled**. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. • **Prevent Adobe Flash Player from running in Office 2010 on affected systems** **Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer. To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps: 1. Create a text file named Disable_Flash.reg with the following contents: Copy Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. 3. **Note** You must restart Internet Explorer for your changes to take effect.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. • **Prevent ActiveX controls from running in Office 2007 and Office 2010** To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps: 1. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 2. Click **ActiveX Settings** in the left-hand pane, and then select **Disable all controls without notifications**. 3. Click **OK** to save your settings. **Impact of workaround.** Office documents that use embedded ActiveX controls may not display as intended.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	How to undo the workaround. To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps: 4. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 5. Click **ActiveX Settings** in the left-hand pane, and then deselect **Disable all controls without notifications**. 6. Click **OK** to save your settings. • **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To raise the browsing security level in Internet Explorer, perform the following steps: 1. On the Internet Explorer **Tools** menu, click **Internet Options**. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Impact of workaround. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". • **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone** You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround.** There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". • **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone. To do this, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	sites that will host the update, and they require an ActiveX control to install the update. **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

ADV170010						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

ADV170010						
Adobe Flash Player on Windows 10 for 32-bit Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170010						
Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170010						
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for 32-bit systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170010						
Adobe Flash Player on Windows 8.1 for x64-based systems	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170010						
Adobe Flash Player on Windows Server 2012 R2	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4034662 (Security Update)	Critical	Remote Code Execution	4033813	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-8673 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8673 MITRE NVD	**CVE Title:** Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the RDP service on the target system to stop responding. To exploit this vulnerability, an attacker would need to run a specially crafted application against a server which provides Remote Desktop Protocol (RDP) services. The update addresses the vulnerability by correcting how RDP handles connection requests. **FAQ:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8673						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Important	Denial of Service	4025342	Base: 5.90 Temporal: 5.30 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 x64-	4034674 (Securit	Important	Denial of Service	4025342	Base: 5.90 Temporal: 5.30 Vector:	Yes

CVE-2017-8673						
based Systems	y Update)				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	

CVE-2017-8674 - Scripting Engine Memory Corruption Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8674 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related 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. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information published.		

Affected Software

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

CVE-2017-8674						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4034674 (Security Update)	Critical	Remote Code Execution	4025342	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4034674	Critical	Remote Code	4025342	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8674						
on Windows 10 Version 1703 for x64-based Systems	(Security 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	

CVE-2017-8691 - Express Compressed Fonts Remote Code Execution Vulnerability

(top)

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8691 MITRE NVD	**CVE Title:** Express Compressed Fonts Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploits exploited this vulnerability would gain code execution on the target system. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. There are multiple ways an attacker could exploit the vulnerability: • In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability and then convince users to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email or Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• In a file sharing attack scenario, an attacker could provide a specially crafted document file that is designed to exploit the vulnerability, and then convince users to open the document file. The security update addresses the vulnerability by correcting how the Windows font library handles embedded fonts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-08-08T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8691						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4034679 (Security Only) 4034664 (Monthly Rollup)	Important	Remote Code Execution	4025341	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8691						
Windows 7 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Remote Code Execution	4025341	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4035056 (Security Update)	Important	Remote Code Execution	None	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8691						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4035056 (Security Update)	Important	Remote Code Execution	None	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based	4035056 (Security Update)	Important	Remote Code Execution	None	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8691						
Systems Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4035056 (Security Update)	Important	Remote Code Execution	None	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4035056 (Securit	Important	Remote Code Execution	None	Base: 5.00 Temporal: 4.50 Vector:	Yes

CVE-2017-8691						
Service Pack 2 (Server Core installation)	y Update)				CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Remote Code Execution	4025341	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8691						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4034664 (Monthly Rollup) 4034679 (Security Only)	Important	Remote Code Execution	4025341	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service	4034664 (Monthly Rollup) 4034679	Important	Remote Code Execution	4025341	Base: 5.00 Temporal: 4.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-8691						
Pack 1 (Server Core installation)	(Security Only)					

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