Microsoft Security Bulletin Summary for May 2016

Published: May 10, 2016 | Updated: May 25, 2016

Version: 2.1

This bulletin summary lists security bulletins released for May 2016.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit Microsoft Technical Security Notifications.

Microsoft also provides information to help customers prioritize monthly security updates with any non-security updates that are being released on the same day as the monthly security updates. Please see the section, **Other Information**.

On this page

Executive Summaries

The following table summarizes the security bulletins for this month in order of severity.

For details on affected software, see the next section, **Affected Software**.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS16-051	**Cumulative Security Update for Internet Explorer (3155533)** This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited the vulnerabilities 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.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Internet Explorer
MS16-052	**Cumulative Security Update for Microsoft Edge (3155538)** This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than users with administrative user rights.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Microsoft Edge
MS16-053	**Cumulative Security Update for JScript and VBScript (3156764)** This security update resolves vulnerabilities in the JScript and VBScript scripting engines in Microsoft Windows. The vulnerabilities could allow remote code execution if a user visits a specially crafted website. An attacker who successfully exploited these vulnerabilities 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 these vulnerabilities could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Critical Remote Code Execution	May require restart	---------	Microsoft Windows
MS16-054	**Security Update for Microsoft Office (3155544)** This security update resolves vulnerabilities in Microsoft Office. The vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Critical Remote Code Execution	May require restart	---------	Microsoft Office, Microsoft Office Services and Web Apps
MS16-055	**Security Update for Microsoft Graphics Component (3156754)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a specially crafted website. 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.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-056	**Security Update for Windows Journal (3156761)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. 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.	Critical Remote Code Execution	May require restart	---------	Microsoft Windows
MS16-057	**Security Update for Windows Shell (3156987)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker successfully convinces a user to browse to a specially crafted website that accepts user-provided online content, or convinces a user to open specially crafted content. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Users whose accounts are configured to have fewer user	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows

	rights on the system could be less impacted than those who operate with administrative user rights.				
MS16-058	**Security Update for Windows IIS (3141083)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker with access to the local system executes a malicious application. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Important Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-059	**Security Update for Windows Media Center (3150220)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Important Remote Code Execution	May require restart	---------	Microsoft Windows
MS16-060	**Security Update for Windows Kernel (3154846)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-061	**Security Update for Microsoft RPC (3155520)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an authenticated attacker makes malformed Remote Procedure Call (RPC) requests to an affected host.	Important Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-062	**Security Update for Windows Kernel-Mode Drivers (3158222)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-064	**Security Update for Adobe Flash Player (3157993)** This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, and Windows 10.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Adobe Flash Player
MS16-065	**Security Update for .NET Framework (3156757)** This security update resolves a vulnerability in Microsoft .NET Framework. The vulnerability could cause information disclosure if an attacker injects unencrypted data into the target secure channel and then performs a man-in-the-middle (MiTM) attack between the targeted client and a legitimate server.	Important Information Disclosure	May require restart	3156757	Microsoft Windows, Microsoft .NET Framework
MS16-066	**Security Update for Virtual Secure Mode (3155451)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker runs a specially crafted application to bypass code integrity protections in Windows.	Important Security Feature Bypass	Requires restart	---------	Microsoft Windows
MS16-067	**Security Update for Volume Manager Driver (3155784)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if a USB disk mounted over Remote Desktop Protocol (RDP) via Microsoft RemoteFX is not correctly tied to the session of the mounting user.	Important Information Disclosure	May require restart	---------	Microsoft Windows

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

How do I use this table?

Use this table to learn about the likelihood of code execution and denial of service exploits within 30 days of security bulletin release, for each of the security updates that you may need to install. Review each of the assessments below, in accordance with your specific configuration, to prioritize your deployment of this month's updates. For more information about what these ratings mean, and how they are determined, please see Microsoft Exploitability Index.

In the columns below, "Latest Software Release" refers to the subject software, and "Older Software Releases" refers to all older, supported releases of the subject software, as listed in the "Affected Software" and "Non-Affected Software" tables in the bulletin.

CVE ID	Vulnerability Title	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment
MS16-051: Cumulative Security Update for Internet Explorer (3155533)				
CVE-2016-0187	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0188	Internet Explorer Security Feature Bypass	3 - Exploitation Unlikely	4 - Not affected	Not applicable

CVE-2016-0189	Scripting Engine Memory Corruption Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
CVE-2016-0192	Microsoft Browser Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0194	Internet Explorer Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-052: Cumulative Security Update for Microsoft Edge (3155538)				
CVE-2016-0186	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0191	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0192	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0193	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-053: Cumulative Security Update for JScript and VBScript (3156764)				
CVE-2016-0187	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0189	Scripting Engine Memory Corruption Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
MS16-054: Security Update for Microsoft Office (3155544)				
CVE-2016-0126	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0140	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-0183	Microsoft Office Graphics RCE Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-0198	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation Less Likely	1 - Exploitation Less Likely	Not applicable
MS16-055: Security Update for Microsoft Graphics Component (3156754)				
CVE-2016-0168	Windows Graphics Component Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Temporary
CVE-2016-0169	Windows Graphics Component Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Temporary
CVE-2016-0170	Windows Graphics Component RCE vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0184	Direct3D Use After Free Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0195	Windows Imaging Component Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-056: Security Update for Windows Journal (3156761)				
CVE-2016-0182	Journal Memory Corruption Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-057: Security Update for Windows Shell (3156987)				
CVE-2016-0179	Windows Shell Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-058: Security Update for Windows IIS (3141083)				
CVE-2016-0152	Windows DLL Loading Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-059: Security Update for Windows Media Center (3150220)				
CVE-2016-0185	Windows Media Center Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-060: Security Update for Windows Kernel (3154846)				
CVE-2016-0180	Windows Kernel Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-061: Security Update for Microsoft RPC (3155520)				
CVE-2016-0178	RPC Network Data Representation Engine Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-062: Security Update for Windows Kernel-Mode Drivers (3158222)				
CVE-2016-0171	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-0173	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

CVE-2016-0174	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-0175	Win32k Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0176	Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0196	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-0197	Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-064: Security Update for Adobe Flash Player (3157993)				
APSB16-15	See Adobe Security Bulletin APSB16-15 for vulnerability severity and update priority ratings.	Not applicable	Not applicable	Not applicable
MS16-065: Security Update for .NET Framework (3156757)				
CVE-2016-0149	TLS/SSL Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-066: Security Update for Virtual Secure Mode (3155451)				
CVE-2016-0181	Hypervisor Code Integrity Security Feature Bypass	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-067: Security Update for Volume Manager Driver (3155784)				
CVE-2016-0190	Remote Desktop Protocol Drive Redirection Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable

Affected Software

The following tables list the bulletins in order of major software category and severity.

Use these tables to learn about the security updates that you may need to install. You should review each software program or component listed to see whether any security updates pertain to your installation. If a software program or component is listed, then the severity rating of the software update is also listed.

Note You may have to install several security updates for a single vulnerability. Review the whole column for each bulletin identifier that is listed to verify the updates that you have to install, based on the programs or components that you have installed on your system.

Windows Operating Systems and Components (Table 1 of 2)

Windows Vista								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Critical**	**None**	**Important**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (3154070) (Critical)	Not applicable	VBScript 5.7 (3158991) (Critical)	Windows Vista Service Pack 2 (3156013) (Critical) Windows Vista Service Pack 2 (3156016) (Critical) Windows Vista Service Pack 2 (3156019) (Critical)	Windows Vista Service Pack 2 (3155178) (Critical)	Not applicable	Windows Vista Service Pack 2 (3141083) (Important)	Windows Vista Service Pack 2 (3150220) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3154070) (Critical)	Not applicable	VBScript 5.7 (3158991) (Critical)	Windows Vista x64 Edition Service Pack 2 (3156013) (Critical)	Windows Vista x64 Edition Service Pack 2 (3155178) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3141083) (Important)	Windows Vista x64 Edition Service Pack 2 (3150220) (Important)

				Windows Vista x64 Edition Service Pack 2 (3156016) (Critical) Windows Vista x64 Edition Service Pack 2 (3156019) (Critical)				
Windows Server 2008								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Moderate**	**None**	**Moderate**	**Critical**	**None**	**None**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (3154070) (Moderate)	Not applicable	VBScript 5.7 (3158991) (Moderate)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3156013) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (3156016) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (3156019) (Critical)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3141083) (Important)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3154070) (Moderate)	Not applicable	VBScript 5.7 (3158991) (Moderate)	Windows Server 2008 for x64-based Systems Service Pack 2 (3156013) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (3156016) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (3156019) (Critical)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3141083) (Important)	Not applicable

Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	VBScript 5.7 (3158991) (Moderate)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3156013) (Critical) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3156019) (Critical)	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3141083) (Important)	Not applicable
Windows 7								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**Critical**	**None**	**None**	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (3154070) (Critical)	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3156013) (Critical) Windows 7 for 32-bit Systems Service Pack 1 (3156016) (Critical) Windows 7 for 32-bit Systems Service Pack 1 (3156019) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3155178) (Critical)	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3150220) (Important)
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (3154070) (Critical)	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3156013) (Critical) Windows 7 for x64-based Systems Service Pack 1 (3156016) (Critical) Windows 7 for x64-based Systems Service Pack 1 (3156019) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3155178) (Critical)	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3150220) (Important)
Windows Server 2008 R2								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**

Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**None**	**None**	**None**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 11 (3154070) (Moderate)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3156013) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3156016) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3156019) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3156013) (Critical) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3156016) (Critical) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3156019) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable
Windows 8.1								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**Critical**	**Critical**	**None**	**Important**
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3154070) (Critical)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (3156013) (Critical) Windows 8.1 for 32-bit Systems (3156016) (Critical)	Windows 8.1 for 32-bit Systems (3155178) (Critical)	Windows 8.1 for 32-bit Systems (3156059) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3150220) (Important)

				Windows 8.1 for 32-bit Systems (3156019) (Critical)				
Windows 8.1 for x64-based Systems	Internet Explorer 11 (3154070) (Critical)	Not applicable	Not applicable	Windows 8.1 for x64-based Systems (3156013) (Critical) Windows 8.1 for x64-based Systems (3156016) (Critical) Windows 8.1 for x64-based Systems (3156019) (Critical)	Windows 8.1 for x64-based Systems (3155178) (Critical)	Windows 8.1 for x64-based Systems (3156059) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3150220) (Important)
Windows Server 2012 and Windows Server 2012 R2								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**None**	**Critical**	**None**	**None**
Windows Server 2012	Internet Explorer 10 (3154070) (Moderate)	Not applicable	Not applicable	Windows Server 2012 (3156013) (Critical) Windows Server 2012 (3156016) (Critical) Windows Server 2012 (3156019) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2	Internet Explorer 11 (3154070) (Moderate)	Not applicable	Not applicable	Windows Server 2012 R2 (3156013) (Critical) Windows Server 2012 R2 (3156016) (Critical) Windows Server 2012 R2 (3156019) (Critical)	Not applicable	Windows Server 2012 R2 (3156059) (Critical)	Not applicable	Not applicable
Windows RT 8.1								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**Critical**	**Critical**	**None**	**None**
Windows RT 8.1	Internet Explorer 11 (3154070) (Critical)	Not applicable	Not applicable	Windows RT 8.1 (3156013) (Critical)	Windows RT 8.1 (3155178) (Critical)	Windows RT 8.1 (3156059) (Critical)	Not applicable	Not applicable

				Windows RT 8.1 (3156016) (Critical) Windows RT 8.1 (3156019) (Critical)				
Windows 10								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**Critical**	**Critical**	**None**	**Critical**	**Critical**	**Critical**	**None**	**None**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3156387) (Critical)	Microsoft Edge (3156387) (Critical)	Not applicable	Windows 10 for 32-bit Systems (3156387) (Critical)	Windows 10 for 32-bit Systems (3156387) (Critical)	Windows 10 for 32-bit Systems (3156387) (Critical)	Not applicable	Not applicable
Windows 10 for x64-based Systems	Internet Explorer 11 (3156387) (Critical)	Microsoft Edge (3156387) (Critical)	Not applicable	Windows 10 for x64-based Systems (3156387) (Critical)	Windows 10 for x64-based Systems (3156387) (Critical)	Windows 10 for x64-based Systems (3156387) (Critical)	Not applicable	Not applicable
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3156421) (Critical)	Microsoft Edge (3156421) (Critical)	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3156421) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3156421) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3156421) (Critical)	Not applicable	Not applicable
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3156421) (Critical)	Microsoft Edge (3156421) (Critical)	Not applicable	Windows 10 Version 1511 for x64-based Systems (3156421) (Critical)	Windows 10 Version 1511 for x64-based Systems (3156421) (Critical)	Windows 10 Version 1511 for x64-based Systems (3156421) (Critical)	Not applicable	Not applicable
Server Core installation option								
Bulletin Identifier	**MS16-051**	**MS16-052**	**MS16-053**	**MS16-055**	**MS16-056**	**MS16-057**	**MS16-058**	**MS16-059**
Aggregate Severity Rating	**None**	**None**	**Moderate**	**Critical**	**None**	**None**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3158991) (Moderate)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3156013) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3156016) (Critical) Windows Server 2008 for 32-bit	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3141083) (Important)	Not applicable

				Systems Service Pack 2 (Server Core installation) (3156019) (Critical)				
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3158991) (Moderate)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3156013) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3156016) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3156019) (Critical)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3141083) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	JScript 5.8 and VBScript 5.8 (3155413) (Moderate)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3156013) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3156016) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	Not applicable	Not applicable

				(3156019) (Critical)				
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3156013) (Critical) Windows Server 2012 (Server Core installation) (3156016) (Critical) Windows Server 2012 (Server Core installation) (3156019) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3156013) (Critical) Windows Server 2012 R2 (Server Core installation) (3156016) (Critical) Windows Server 2012 R2 (Server Core installation) (3156019) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**None**	**None**
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (3153171) (Important)	Windows Vista Service Pack 2 (3153171) (Important)	Windows Vista Service Pack 2 (3153199) (Important) Windows Vista Service Pack 2 (3156017) (Important)	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (3142023) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important)	Not applicable	Not applicable

					Microsoft .NET Framework 4.6 (3142037) (Important)		
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3153171) (Important)	Windows Vista x64 Edition Service Pack 2 (3153171) (Important)	Windows Vista x64 Edition Service Pack 2 (3153199) (Important) Windows Vista x64 Edition Service Pack 2 (3156017) (Important)	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (3142023) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6 (3142037) (Important)	Not applicable	Not applicable
Windows Server 2008							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3153171) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3153171) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3153199) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3156017) (Important)	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (3142023) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6 (3142037) (Important)	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (3153171) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3153171) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3153199) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3156017) (Important)	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (3142023) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6 (3142037) (Important)	Not applicable	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3153171) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3153171) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3153199) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (3142023) (Important)	Not applicable	Not applicable

			(3156017) (Important)				
Windows 7							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**None**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Windows 7 for 32-bit Systems Service Pack 1 (3153171) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3153171) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3153199) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3156017) (Important)	Not applicable	Microsoft .NET Framework 3.5.1 (3142024) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142037) (Important)	Not applicable	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Windows 7 for x64-based Systems Service Pack 1 (3153171) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3153171) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3153199) (Important) Windows 7 for x64-based Systems Service Pack 1 (3156017) (Important)	Not applicable	Microsoft .NET Framework 3.5.1 (3142024) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142037) (Important)	Not applicable	Not applicable
Windows Server 2008 R2							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**None**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3153171) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3153171) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3153199) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3156017) (Important)	Not applicable	Microsoft .NET Framework 3.5.1 (3142024) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142037) (Important)	Not applicable	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Windows Server 2008 R2 for Itanium-based	Windows Server 2008 R2 for Itanium-based	Windows Server 2008 R2 for Itanium-based	Not applicable	Microsoft .NET Framework	Not applicable	Not applicable

	Systems Service Pack 1 (3153171) (Important)	Systems Service Pack 1 (3153171) (Important)	Systems Service Pack 1 (3153199) (Important) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3156017) (Important)		3.5.1 (3142024) (Important)		
Windows 8.1							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Important**	**None**	**None**
Windows 8.1 for 32-bit Systems	Windows 8.1 for 32-bit Systems (3153171) (Important)	Windows 8.1 for 32-bit Systems (3153704) (Important)	Windows 8.1 for 32-bit Systems (3153199) (Important) Windows 8.1 for 32-bit Systems (3156017) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 3.5 (3142026) (Important) Microsoft .NET Framework 4.5.2 (3142030) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142036) (Important)	Not applicable	Not applicable
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3153171) (Important)	Windows 8.1 for x64-based Systems (3153704) (Important)	Windows 8.1 for x64-based Systems (3153199) (Important) Windows 8.1 for x64-based Systems (3156017) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 3.5 (3142026) (Important) Microsoft .NET Framework 4.5.2 (3142030) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142036) (Important)	Not applicable	Not applicable
Windows Server 2012 and Windows Server 2012 R2							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Moderate**	**Important**	**None**	**Important**
Windows Server 2012	Windows Server 2012 (3153171) (Important)	Windows Server 2012 (3153704) (Important)	Windows Server 2012 (3153199) (Important) Windows Server 2012 (3156017) (Important)	Adobe Flash Player (3163207) (Moderate)	Microsoft .NET Framework 3.5 (3142025) (Important) Microsoft .NET Framework 4.5.2 (3142032) (Important) Microsoft .NET Framework 4.6/4.6.1	Not applicable	Windows Server 2012 (3155784) (Important)

					(3142035) (Important)		
Windows Server 2012 R2	Windows Server 2012 R2 (3153171) (Important)	Windows Server 2012 R2 (3153704) (Important)	Windows Server 2012 R2 (3153199) (Important) Windows Server 2012 R2 (3156017) (Important)	Adobe Flash Player (3163207) (Moderate)	Microsoft .NET Framework 3.5 (3142026) (Important) Microsoft .NET Framework 4.5.2 (3142030) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142036) (Important)	Not applicable	Windows Server 2012 R2 (3155784) (Important)
Windows RT 8.1							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Important**	**None**	**None**
Windows RT 8.1	Windows RT 8.1 (3153171) (Important)	Windows RT 8.1 (3153704) (Important)	Windows RT 8.1 (3153199) (Important) Windows RT 8.1 (3156017) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 4.5.2 (3142030) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142036) (Important)	Not applicable	Not applicable
Windows 10							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Important**	**Important**	**None**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3156387) (Important)	Windows 10 for 32-bit Systems (3156387) (Important)	Windows 10 for 32-bit Systems (3156387) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 3.5 (3156387) (Important) Microsoft .NET Framework 4.6 (3156387) (Important)	Windows 10 for 32-bit Systems (3156387) (Important)	Not applicable
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3156387) (Important)	Windows 10 for x64-based Systems (3156387) (Important)	Windows 10 for x64-based Systems (3156387) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 3.5 (3156387) (Important) Microsoft .NET Framework 4.6 (3156387) (Important)	Windows 10 for x64-based Systems (3156387) (Important)	Not applicable
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3156421) (Important)	Windows 10 Version 1511 for 32-bit Systems (3156421) (Important)	Windows 10 Version 1511 for 32-bit Systems (3156421) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 3.5 (3156421) (Important) Microsoft .NET	Windows 10 Version 1511 for 32-bit Systems (3156421) (Important)	Not applicable

					Framework 4.6.1 (3156421) (Important)		
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3156421) (Important)	Windows 10 Version 1511 for x64-based Systems (3156421) (Important)	Windows 10 Version 1511 for x64-based Systems (3156421) (Important)	Adobe Flash Player (3163207) (Critical)	Microsoft .NET Framework 3.5 (3156421) (Important) Microsoft .NET Framework 4.6.1 (3156421) (Important)	Windows 10 Version 1511 for x64-based Systems (3156421) (Important)	Not applicable
Server Core installation option							
Bulletin Identifier	**MS16-060**	**MS16-061**	**MS16-062**	**MS16-064**	**MS16-065**	**MS16-066**	**MS16-067**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**None**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3153171) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3153171) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3153199) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3156017) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3153171) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3153171) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3153199) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3156017) (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3153171) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3153171) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3153199) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3156017) (Important)	Not applicable	Microsoft .NET Framework 3.5.1 (3142024) (Important) Microsoft .NET Framework 4.5.2 (3142033) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142037) (Important)	Not applicable	Not applicable
Windows Server 2012 (Server Core installation)	Windows Server 2012	Windows Server 2012	Windows Server 2012	Not applicable	Microsoft .NET	Not applicable	Windows Server 2012

	(Server Core installation) (3153171) (Important)	(Server Core installation) (3153704) (Important)	(Server Core installation) (3153199) (Important) Windows Server 2012 (Server Core installation) (3156017) (Important)		Framework 3.5 (3142025) (Important) Microsoft .NET Framework 4.5.2 (3142032) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142035) (Important)		(Server Core installation) (3155784) (Important)
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3153171) (Important)	Windows Server 2012 R2 (Server Core installation) (3153704) (Important)	Windows Server 2012 R2 (Server Core installation) (3153199) (Important) Windows Server 2012 R2 (Server Core installation) (3156017) (Important)	Not applicable	Microsoft .NET Framework 3.5 (3142026) (Important) Microsoft .NET Framework 4.5.2 (3142030) (Important) Microsoft .NET Framework 4.6/4.6.1 (3142036) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3155784) (Important)

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (2984938) (Important) Microsoft Office 2007 Service Pack 3 (2984943) (Important) Microsoft Word 2007 Service Pack 3 (3115116) (Critical)
Microsoft Office 2010	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3115121) (Critical) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3054984) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3101520) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3115123) (Critical)

Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3115121) (Critical) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3054984) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3101520) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3115123) (Critical)
Microsoft Office 2013	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Office 2013 Service Pack 1 (32-bit editions) (3115016) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3115025) (Critical)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Office 2013 Service Pack 1 (64-bit editions) (3115016) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3115025) (Critical)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 RT Service Pack 1	Microsoft Office 2013 RT Service Pack 1 (3115016) (Important) Microsoft Word 2013 RT Service Pack 1 (3115025) (Critical)
Microsoft Office 2016	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 (32-bit edition)	Microsoft Office 2016 (32-bit edition) (3115103) (Important) Microsoft Word 2016 (32-bit edition) (3115094) (Critical)
Microsoft Office 2016 (64-bit edition)	Microsoft Office 2016 (64-bit edition) (3115103) (Important) Microsoft Word 2016 (64-bit edition) (3115094) (Critical)
Microsoft Office for Mac 2011	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office for Mac 2011	Microsoft Word for Mac 2011 (3155776)

	(Critical)
Microsoft Office 2016 for Mac	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 for Mac	Microsoft Word 2016 for Mac (3155777) (Critical)
Other Office Software	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3115115) (Critical)
Microsoft Word Viewer	Microsoft Word Viewer (3115132) (Critical)

Note for MS16-054

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft SharePoint Server 2010 Service Pack 2	Word Automation Services (3115117) (Critical)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-054**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3115124) (Critical)

Note for MS16-054

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Detection and Deployment Tools and Guidance

Several resources are available to help administrators deploy security updates.

Microsoft Baseline Security Analyzer (MBSA) lets administrators scan local and remote systems for missing security updates and common security misconfigurations.

Windows Server Update Services (WSUS), Systems Management Server (SMS), and System Center Configuration Manager help administrators distribute security updates.

The Update Compatibility Evaluator components included with Application Compatibility Toolkit aid in streamlining the testing and validation of Windows updates against installed applications.

For information about these and other tools that are available, see Security Tools for IT Pros.

Acknowledgments

Microsoft recognizes the efforts of those in the security community who help us protect customers through responsible vulnerability disclosure. See Acknowledgments for more information.

Other Information

Microsoft Windows Malicious Software Removal Tool

For the bulletin release that occurs on the second Tuesday of each month, Microsoft has released an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Update, Microsoft Update, Windows Server Update Services, and the Download Center. No updated version of the Microsoft Windows Malicious Software Removal Tool is available for out-of-band security bulletin releases.

Non-Security Updates on MU, WU, and WSUS

For information about non-security releases on Windows Update and Microsoft Update, please see:

- Microsoft Knowledge Base Article 894199: Description of Software Update Services and Windows Server Update Services changes in content. Includes all Windows content.
- Updates from Past Months for Windows Server Update Services. Displays all new, revised, and rereleased updates for Microsoft products other than Microsoft Windows.

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections websites provided by program partners listed in Microsoft Active Protections Program (MAPP) Partners.

Security Strategies and Community

Update Management Strategies

Security Guidance for Update Management provides additional information about Microsoft's best-practice recommendations for applying security updates.

Obtaining Other Security Updates

Updates for other security issues are available from the following locations:

- Security updates are available from Microsoft Download Center. You can find them most easily by doing a keyword search for "security update".
- Updates for consumer platforms are available from Microsoft Update.
- You can obtain the security updates offered this month on Windows Update, from Download Center on Security and Critical Releases ISO CD Image files. For more information, see Microsoft Knowledge Base Article 913086.

IT Pro Security Community

Learn to improve security and optimize your IT infrastructure, and participate with other IT Pros on security topics in IT Pro Security Community.

Support

The affected software listed has been tested to determine which versions are affected. Other versions are past their support life cycle. To determine the support life cycle for your software version, visit Microsoft Support Lifecycle.

Security solutions for IT professionals: TechNet Security Troubleshooting and Support

Help protect your computer that is running Windows from viruses and malware: Virus Solution and Security Center

Local support according to your country: International Support

Disclaimer

Revisions

- V1.0 (May 10, 2016): Bulletin Summary published.
- V1.1 (May 11, 2016): Bulletin Summary revised to change the vulnerability impact of MS16-061 from elevation of privilege to remote code execution, and the title of CVE 2016-0178 to RPC Network Data Representation Engine Remote Code Execution Vulnerability. This is an informational change only.
- V1.2 (May 13, 2016): For MS16-067, Bulletin Summary revised to change the vulnerability severity rating for Windows 8.1 and Windows RT 8.1 to Not applicable, because these operating systems are not affected by the vulnerability described in this bulletin. Customers who have applied security update 3155784 do not need to take any further action. This is an informational change only.
- V2.0 (May 13, 2016): For MS16-064, Bulletin Summary revised to announce the release of update 3163207 to address the vulnerabilities included in Adobe Security Bulletin APSB16-15. Note that update 3163207 replaces the update previously released in MS16-064 (update 3157993). Microsoft strongly recommends that customers install update 3163207 to help be protected from the vulnerabilities described in Adobe Security Bulletin APSB16-15.
- V2.1 (May 25, 2016): For MS16-065, added a Known Issue to the Executive Summaries table. After you install any of the security updates that are included in MS16-065 on a Front End or Standard Edition server for Lync Server 2010, Lync Server 2013, or Skype for Business Server 2015, several conferencing modalities no longer function for internal users. For information about the solution for this Known Issue, see Microsoft Knowledge Base Article 3165438.

Page generated 2016-05-25 12:52-07:00.