EN Ez a tartalom nem érhető el az Ön nyelvén, csak angol nyelven.

Microsoft Security Bulletin Summary for June 2016

Published: June 14, 2016 | Updated: August 9, 2016

Version: 2.2

This bulletin summary lists security bulletins released for June 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
MS16-063	**Cumulative Security Update for Internet Explorer (3163649)** 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
MS16-068	**Cumulative Security Update for Microsoft Edge (3163656)** 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
MS16-069	**Cumulative Security Update for JScript and VBScript (3163640)** This security update resolves vulnerabilities in the JScript and VBScript scripting engines in Microsoft Windows. The vulnerabilities	Critical Remote Code Execution	May require restart	---------	Microsoft Windows

	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.				
MS16-070	**Security Update for Microsoft Office (3163610)** This security update resolves vulnerabilities in Microsoft Office. The most severe of 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
MS16-071	**Security Update for Microsoft Windows DNS Server (3164065)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker sends specially crafted requests to a DNS server.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-072	**Security Update for Group Policy (3163622)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker launches a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine.	Important Elevation of Privilege	Requires restart	3159398	Microsoft Windows
MS16-073	**Security Update for Windows Kernel-Mode Drivers (3164028)** This security update resolves vulnerabilities in Microsoft Windows. The most 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
MS16-074	**Security Update for Microsoft Graphics Component (3164036)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow elevation of privilege if a user opens a specially crafted application.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-075	**Security Update for Windows SMB Server (3164038)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an	Important Elevation of Privilege	Requires restart	3161561	Microsoft Windows

	attacker logs on to the system and runs a specially crafted application.				
MS16-076	**Security Update for Netlogon (3167691)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker with access to a domain controller (DC) on a target network runs a specially crafted application to establish a secure channel to the DC as a replica domain controller.	Important Remote Code Execution	Requires restart	3161561	Microsoft Windows
MS16-077	**Security Update for WPAD (3165191)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if the Web Proxy Auto Discovery (WPAD) protocol falls back to a vulnerable proxy discovery process on a target system.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-078	**Security Update for Windows Diagnostic Hub (3165479)** 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
MS16-079	**Security Update for Microsoft Exchange Server (3160339)** This security update resolves vulnerabilities in Microsoft Exchange Server. The most severe of the vulnerabilities could allow information disclosure if an attacker sends a specially crafted image URL in an Outlook Web Access (OWA) message that is loaded, without warning or filtering, from the attacker-controlled URL.	Important Information Disclosure	May require restart	---------	Microsoft Exchange Server
MS16-080	**Security Update for Microsoft Windows PDF (3164302)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted .pdf file. An attacker who successfully exploited the vulnerabilities could cause arbitrary code to execute in the context of the current user. However, an attacker would have no way to force a user to open a specially crafted .pdf file.	Important Remote Code Execution	May require restart	---------	Microsoft Windows
MS16-081	**Security Update for Active Directory (3160352)** This security update resolves a vulnerability in Active Directory. The vulnerability could allow denial of service if an authenticated attacker creates multiple machine accounts. To exploit the vulnerability an attacker must have an account that has privileges to join machines to the domain.	Important Denial of Service	Requires restart	---------	Microsoft Windows
MS16-082	**Security Update for Microsoft Windows Search Component (3165270)** This security update resolves a vulnerability	Important Denial of Service	Requires restart	---------	Microsoft Windows

	in Microsoft Windows. The vulnerability could allow denial of service if an attacker logs on to a target system and runs a specially crafted application.				
MS16-083	**Security Update for Adobe Flash Player (3167685)** 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

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
MS16-063: Cumulative Security Update for Internet Explorer (3163649)				
CVE-2016-0199	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0200	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3202	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3205	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3206	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3207	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3210	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3211	Internet Explorer	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

	Memory Corruption Vulnerability			
CVE-2016-3212	Internet Explorer XSS Filter Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3213	WPAD Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-068: Cumulative Security Update for Microsoft Edge (3163656)				
CVE-2016-3198	Microsoft Edge Security Feature Bypass	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-3199	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3201	Windows PDF Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3202	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3203	Windows PDF Remote Code Execution Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3214	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3215	Windows PDF Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3222	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-069: Cumulative Security Update for JScript and VBScript (3163640)				
CVE-2016-3205	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3206	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3207	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-070: Security Update for Microsoft Office (3163610)				
CVE-2016-0025	Microsoft Office	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

	Memory Corruption Vulnerability			
CVE-2016-3233	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-3234	Microsoft Office Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3235	Microsoft Office OLE DLL Side Loading Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-071: Security Update for Microsoft Windows DNS Server (3164065)				
CVE-2016-3227	Windows DNS Server Use After Free Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Permanent
MS16-072: Security Update for Group Policy (3163622)				
CVE-2016-3223	Group Policy Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-073: Security Update for Windows Kernel-Mode Drivers (3164028)				
CVE-2016-3218	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-3221	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-3232	Windows Virtual PCI Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-074: Security Update for Microsoft Graphics Component (3164036)				
CVE-2016-3216	Windows Graphics Component Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3219	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3220	ATMFD.DLL Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-075: Security Update for Windows SMB Server (3164038)				
CVE-2016-3225	Windows SMB	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable

	Server Elevation of Privilege Vulnerability			
MS16-076: Security Update for Netlogon (3167691)				
CVE-2016-3228	Windows Netlogon Memory Corruption Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-077: Security Update for WPAD (3165191)				
CVE-2016-3213	Windows WPAD Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3236	Windows WPAD Proxy Discovery Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3299	NetBIOS Spoofing Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-078: Security Update for Windows Diagnostic Hub (3165479)				
CVE-2016-3231	Windows Diagnostics Hub Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-079: Security Update for Microsoft Exchange Server (3160339)				
CVE-2016-0028	Microsoft Exchange Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-080: Security Update for Microsoft Windows PDF (3164302)				
CVE-2016-3201	Windows PDF Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3203	Windows PDF Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3215	Windows PDF Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-081: Security Update for Active Directory (3160352)				
CVE-2016-3226	Active Directory Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent

MS16-082: Security Update for Microsoft Windows Search Component (3165270)				
CVE-2016-3230	Windows Search Component Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
MS16-083: Security Update for Adobe Flash Player (3167685)				
APSB16-18	See Adobe Security Bulletin APSB16-18 for vulnerability severity and update priority ratings.	Not applicable	Not applicable	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	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**None**	**Important**	**Important**	**Important**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (3160005) (Critical)	Not applicable	VBScript 5.7 (3158364) (Critical)	Not applicable	Windows Vista Service Pack 2 (3159398) (Important)	Windows Vista Service Pack 2 (3161664) (Important)	Windows Vista Service Pack 2 (3164033) (Important) Windows Vista Service Pack 2 (3164035) (Important)	Windows Vista Service Pack 2 (3161561) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3160005) (Critical)	Not applicable	VBScript 5.7 (3158364) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3159398) (Important)	Windows Vista x64 Edition Service Pack 2 (3161664) (Important)	Windows Vista x64 Edition Service Pack 2 (3164033) (Important) Windows	Windows Vista x64 Edition Service Pack 2 (3161561) (Important)

							Vista x64 Edition Service Pack 2 (3164035) (Important)	
Windows Server 2008								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Moderate**	**None**	**Moderate**	**None**	**Important**	**Important**	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (3160005) (Moderate)	Not applicable	VBScript 5.7 (3158364) (Moderate)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3159398) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3161664) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3164033) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3164035) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3161561) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3160005) (Moderate)	Not applicable	VBScript 5.7 (3158364) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3159398) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3161664) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3164033) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3164035) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3161561) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	VBScript 5.7 (3158364) (Moderate)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3159398) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3161664) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3164033) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3161561) (Important)

							Windows Server 2008 for Itanium-based Systems Service Pack 2 (3164035) (Important)	
Windows 7								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Critical**	**None**	**None**	**None**	**Important**	**Important**	**Important**	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (3160005) (Critical)	Not applicable	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3159398) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3161664) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3164033) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3164035) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3161561) (Important)
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (3160005) (Critical)	Not applicable	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3159398) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3161664) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3164033) (Important) Windows 7 for x64-based Systems Service Pack 1 (3164035) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3161561) (Important)
Windows Server 2008 R2								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**None**	**Important**	**Important**	**Important**	**Important**
Windows Server 2008 R2 for	Internet Explorer 11	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for	Windows Server 2008 R2 for	Windows Server 2008 R2 for	Windows Server 2008 R2 for

x64-based Systems Service Pack 1	(3160005) (Moderate)				x64-based Systems Service Pack 1 (3159398) (Important)	x64-based Systems Service Pack 1 (3161664) (Important)	x64-based Systems Service Pack 1 (3164033) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3164035) (Important)	x64-based Systems Service Pack 1 (3161561) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3159398) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3161664) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3164033) (Important) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3164035) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3161561) (Important)
Windows 8.1								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Critical**	**None**	**None**	**None**	**Important**	**Important**	**Important**	**Important**
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3160005) (Critical)	Not applicable	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (3159398) (Important)	Windows 8.1 for 32-bit Systems (3161664) (Important)	Windows 8.1 for 32-bit Systems (3164033) (Important) Windows 8.1 for 32-bit Systems (3164035) (Important)	Windows 8.1 for 32-bit Systems (3161561) (Important)
Windows 8.1 for x64-based Systems	Internet Explorer 11 (3160005) (Critical)	Not applicable	Not applicable	Not applicable	Windows 8.1 for x64-based Systems (3159398) (Important)	Windows 8.1 for x64-based Systems (3161664) (Important)	Windows 8.1 for x64-based Systems (3164033) (Important)	Windows 8.1 for x64-based Systems (3161561) (Important)

							Windows 8.1 for x64-based Systems (3164035) (Important)	
Windows Server 2012 and Windows Server 2012 R2								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**Important**	**Important**	**Important**	**Important**
Windows Server 2012	Internet Explorer 10 (3160005) (Moderate)	Not applicable	Not applicable	Windows Server 2012 (3161951) (Critical)	Windows Server 2012 (3159398) (Important)	Windows Server 2012 (3161664) (Important) Windows Server 2012 (3164294) (Important)	Windows Server 2012 (3164033) (Important) Windows Server 2012 (3164035) (Important)	Windows Server 2012 (3161561) (Important)
Windows Server 2012 R2	Internet Explorer 11 (3160005) (Moderate)	Not applicable	Not applicable	Windows Server 2012 R2 (3161951) (Critical)	Windows Server 2012 R2 (3159398) (Important)	Windows Server 2012 R2 (3161664) (Important) Windows Server 2012 R2 (3164294) (Important)	Windows Server 2012 R2 (3164033) (Important) Windows Server 2012 R2 (3164035) (Important)	Windows Server 2012 R2 (3161561) (Important)
Windows RT 8.1								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**Critical**	**None**	**None**	**None**	**Important**	**Important**	**Important**	**Important**
Windows RT 8.1	Internet Explorer 11 (3160005) (Critical)	Not applicable	Not applicable	Not applicable	Windows RT 8.1 (3159398) (Important)	Windows RT 8.1 (3161664) (Important)	Windows RT 8.1 (3164033) (Important) Windows RT 8.1 (3164035) (Important)	Windows RT 8.1 (3161561) (Important)
Windows 10								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity	**Critical**	**Critical**	**None**	**None**	**Important**	**Important**	**Important**	**Important**

Rating								
Windows 10 for 32-bit Systems	Internet Explorer 11 (3163017) (Critical)	Microsoft Edge (3163017) (Critical)	Not applicable	Not applicable	Windows 10 for 32-bit Systems (3163017) (Important)	Windows 10 for 32-bit Systems (3163017) (Important)	Windows 10 for 32-bit Systems (3163017) (Important)	Windows 10 for 32-bit Systems (3163017) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (3163017) (Critical)	Microsoft Edge (3163017) (Critical)	Not applicable	Not applicable	Windows 10 for x64-based Systems (3163017) (Important)	Windows 10 for x64-based Systems (3163017) (Important)	Windows 10 for x64-based Systems (3163017) (Important)	Windows 10 for x64-based Systems (3163017) (Important)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3163018) (Critical)	Microsoft Edge (3163018) (Critical)	Not applicable	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3163018) (Critical)	Microsoft Edge (3163018) (Critical)	Not applicable	Not applicable	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)
Server Core installation option								
Bulletin Identifier	**MS16-063**	**MS16-068**	**MS16-069**	**MS16-071**	**MS16-072**	**MS16-073**	**MS16-074**	**MS16-075**
Aggregate Severity Rating	**None**	**None**	**Moderate**	**Critical**	**Important**	**Important**	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3158364) (Moderate)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3159398) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3161664) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3164033) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3164035) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3161561) (Important)

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3158364) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3159398) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3161664) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3164033) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3164035) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3161561) (Important)
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 (3158363) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3159398) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3161664) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3164033) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3164035) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3161561) (Important)
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3161951) (Critical)	Windows Server 2012 (Server Core installation) (3159398) (Important)	Windows Server 2012 (Server Core installation) (3161664) (Important) Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3164033) (Important) Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3161561) (Important)

						(3164294) (Important)	(3164035) (Important)	
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3161951) (Critical)	Windows Server 2012 R2 (Server Core installation) (3159398) (Important)	Windows Server 2012 R2 (Server Core installation) (3161664) (Important) Windows Server 2012 R2 (Server Core installation) (3164294) (Important)	Windows Server 2012 R2 (Server Core installation) (3164033) (Important) Windows Server 2012 R2 (Server Core installation) (3164035) (Important)	Windows Server 2012 R2 (Server Core installation) (3161561) (Important)

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**	**None**	**None**	**None**
Windows Vista Service Pack 2	Not applicable	Windows Vista Service Pack 2 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Vista x64 Edition Service Pack 2	Not applicable	Windows Vista x64 Edition Service Pack 2 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2008							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**None**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3161561) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server	Windows	Windows	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

2008 for x64-based Systems Service Pack 2	Server 2008 for x64-based Systems Service Pack 2 (3161561) (Important)	Server 2008 for x64-based Systems Service Pack 2 (3161949) (Important)					
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3161561) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows 7							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**	**None**	**Important**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3161958) (Important)	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3161958) (Important)	Not applicable
Windows Server 2008 R2							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**Important**	**Important**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3161561) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3161949) (Important)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3160352) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3161958) (Important)	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Windows Server 2008 R2 for Itanium-based Systems	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable

	(3161561) (Important)	Service Pack 1 (3161949) (Important)				(3161958) (Important)	
Windows 8.1							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**None**	**Important**	**None**	**Important**	**None**	**Important**	**Critical**
Windows 8.1 for 32-bit Systems	Not applicable	Windows 8.1 for 32-bit Systems (3161949) (Important)	Not applicable	Windows 8.1 for 32-bit Systems (3157569) (Important)	Not applicable	Windows 8.1 for 32-bit Systems (3161958) (Important)	Adobe Flash Player (3167685) (Critical)
Windows 8.1 for x64-based Systems	Not applicable	Windows 8.1 for x64-based Systems (3161949) (Important)	Not applicable	Windows 8.1 for x64-based Systems (3157569) (Important)	Not applicable	Windows 8.1 for x64-based Systems (3161958) (Important)	Adobe Flash Player (3167685) (Critical)
Windows Server 2012 and Windows Server 2012 R2							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**Important**	**Important**	**None**	**Important**	**Important**	**Important**	**Moderate**
Windows Server 2012	Windows Server 2012 (3161561) (Important)	Windows Server 2012 (3161949) (Important)	Not applicable	Windows Server 2012 (3157569) (Important)	Windows Server 2012 (3160352) (Important)	Windows Server 2012 (3161958) (Important)	Adobe Flash Player (3167685) (Moderate)
Windows Server 2012 R2	Windows Server 2012 R2 (3162343) (Important)	Windows Server 2012 R2 (3161949) (Important)	Not applicable	Windows Server 2012 R2 (3157569) (Important)	Windows Server 2012 R2 (3160352) (Important)	Windows Server 2012 R2 (3161958) (Important)	Adobe Flash Player (3167685) (Moderate)
Windows RT 8.1							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**	**None**	**Important**	**Critical**
Windows RT 8.1	Not applicable	Windows RT 8.1 (3161949) (Important)	Not applicable	Not applicable	Not applicable	Windows RT 8.1 (3161958) (Important)	Adobe Flash Player (3167685) (Critical)
Windows 10							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**None**	**Important**	**Important**	**Important**	**None**	**Important**	**Critical**
Windows 10 for 32-bit Systems	Not applicable	Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems	Not applicable	Windows 10 for 32-bit Systems	Adobe Flash Player

		(3163017) (Important)	(3163017) (Important)	(3163017) (Important)		(3163017) (Important)	(3167685) (Critical)
Windows 10 for x64-based Systems	Not applicable	Windows 10 for x64-based Systems (3163017) (Important)	Windows 10 for x64-based Systems (3163017) (Important)	Windows 10 for x64-based Systems (3163017) (Important)	Not applicable	Windows 10 for x64-based Systems (3163017) (Important)	Adobe Flash Player (3167685) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3163018) (Important)	Adobe Flash Player (3167685) (Critical)
Windows 10 Version 1511 for x64-based Systems	Not applicable	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Not applicable	Windows 10 Version 1511 for x64-based Systems (3163018) (Important)	Adobe Flash Player (3167685) (Critical)
Server Core installation option							
Bulletin Identifier	**MS16-076**	**MS16-077**	**MS16-078**	**MS16-080**	**MS16-081**	**MS16-082**	**MS16-083**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**Important**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3161949) (Important)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3161949) (Important)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3161949) (Important)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3160352) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3161958) (Important)	Not applicable

Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3161561) (Important)	Windows Server 2012 (Server Core installation) (3161949) (Important)	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3160352) (Important)	Windows Server 2012 (Server Core installation) (3161958) (Important)	Not applicable
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3162343) (Important)	Windows Server 2012 R2 (Server Core installation) (3161949) (Important)	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3160352) (Important)	Windows Server 2012 R2 (Server Core installation) (3161958) (Important)	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Excel 2007 Service Pack 3 (3115107) (Important) Microsoft Visio 2007 Service Pack 3 (3114740) (Important) Microsoft Word 2007 Service Pack 3 (3115195) (Critical)
Microsoft Office 2010	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3115198) (Critical) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3115130) (Important) Microsoft Visio 2010 Service Pack 2 (32-bit editions) (3114872) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3115243) (Critical)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3115198) (Critical)

	Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3115130) (Important) Microsoft Visio 2010 Service Pack 2 (64-bit editions) (3114872) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3115243) (Critical)
Microsoft Office 2013	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Visio 2013 Service Pack 1 (32-bit editions) (3115020) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3115173) (Critical)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Visio 2013 Service Pack 1 (64-bit editions) (3115020) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3115173) (Critical)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 RT Service Pack 1	Microsoft Word 2013 RT Service Pack 1 (3115173) (Critical)
Microsoft Office 2016	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 (32-bit edition)	Microsoft Office 2016 (32-bit edition) (3115144) (Important) Microsoft Visio 2016 (32-bit edition) (3115041) (Important) Microsoft Word 2016 (32-bit edition) (3115182) (Critical)
Microsoft Office 2016 (64-bit edition)	Microsoft Office 2016 (64-bit edition) (3115144) (Important)

	Microsoft Visio 2016 (64-bit edition) (3115041) (Important) Microsoft Word 2016 (64-bit edition) (3115182) (Critical)
Microsoft Office for Mac 2011	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office for Mac 2011	Microsoft Word for Mac 2011 (3165796) (Critical)
Microsoft Office 2016 for Mac	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 for Mac	Microsoft Word 2016 for Mac (3165798) (Critical)
Other Office Software	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Important**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3115111) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3115194) (Important)
Microsoft Visio Viewer 2007 Service Pack 3	Microsoft Visio Viewer 2007 Service Pack 3 (2596915) (Important)
Microsoft Visio Viewer 2010 (32-bit Edition)	Microsoft Visio Viewer 2010 (32-bit Edition) (2999465) (Important)
Microsoft Visio Viewer 2010 (64-bit Edition)	Microsoft Visio Viewer 2010 (64-bit Edition) (2999465) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3115187) (Important)

Note for MS16-070

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	**MS16-070**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Word Automation Services (3115196) (Important)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2013 Service Pack 1	Word Automation Services (3115014) (Important)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3115244) (Important)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3115170) (Important)
Office Online Server	
Bulletin Identifier	**MS16-070**
Aggregate Severity Rating	**Important**
Office Online Server	Office Online Server (3115134) (Important)

Note for MS16-070

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

Microsoft Server Software

Microsoft Exchange Server 2007	
Bulletin Identifier	**MS16-079**
Aggregate Severity Rating	**Important**

Microsoft Exchange Server 2007 Service Pack 3	Microsoft Exchange Server 2007 Service Pack 3 (3151086) (Important)
Microsoft Exchange Server 2010	
Bulletin Identifier	**MS16-079**
Aggregate Severity Rating	**Important**
Microsoft Exchange Server 2010 Service Pack 3	Microsoft Exchange Server 2010 Service Pack 3 (3151097) (Important)
Microsoft Exchange Server 2013	
Bulletin Identifier	**MS16-079**
Aggregate Severity Rating	**Important**
Microsoft Exchange Server 2013 Service Pack 1	Microsoft Exchange Server 2013 Service Pack 1 (3150501) (Important)
Microsoft Exchange Server 2013 Cumulative Update 11	Microsoft Exchange Server 2013 Cumulative Update 11 (3150501) (Important)
Microsoft Exchange Server 2013 Cumulative Update 12	Microsoft Exchange Server 2013 Cumulative Update 12 (3150501) (Important)
Microsoft Exchange Server 2016	
Bulletin Identifier	**MS16-079**
Aggregate Severity Rating	**Important**
Microsoft Exchange Server 2016	Microsoft Exchange Server 2016 (3150501) (Important)
Microsoft Exchange Server 2016 Cumulative Update 1	Microsoft Exchange Server 2016 Cumulative Update 1 (3150501) (Important)

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

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (June 14, 2016): Bulletin Summary published.
- V1.1 (June 15, 2016): For MS16-072, added a Known Issue to the Executive Summaries table. The updates in MS16-072 change the security context with which user group policies are retrieved. For more information about this by-design behavior change, see Microsoft Knowledge Base Article 3163622. For MS16-074, revised the Executive Summary to correct the attack vector description. This is an informational change only.
- V2.0 (June 16, 2016): Bulletin Summary revised to document the out-of-band release of MS16-083.
- V2.1 (June 22, 2016): For MS16-075 and MS16-076, added a Known Issue to the Executive Summaries table for update 3161561. When you try to access a domain DFS namespace (such as \\contoso.com\SYSVOL) on a computer that is configured to require mutual authentication (by using the UNC Hardened Access feature), you receive an "Access Denied" error message. Microsoft is researching this problem and will post more information in this article when it becomes available. For more information, see Microsoft Knowledge Base Article 3161561.
- V2.2 (August 09, 2016): For MS16-077, bulletin revised to include an additional vulnerability, CVE-2016-3299. This is an informational change only. Customers who have successfully installed the updates do not need to take any further action.

Page generated 2016-10-27 11:01-07:00.