Microsoft Security Bulletin Summary for July 2016

Published: July 12, 2016 | Updated: September 12, 2017

Version: 2.0

This bulletin summary lists security bulletins released for July 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 **Affected Software** section.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS16-084	**Cumulative Security Update for Internet Explorer (3169991)** 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
MS16-085	**Cumulative Security Update for Microsoft Edge (3169999)** 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
MS16-086	**Cumulative Security Update for JScript and VBScript (3169996)**	Critical Remote Code Execution	May require restart	---------	Microsoft Windows

	This security update resolves a vulnerability in the JScript and VBScript scripting engines in Microsoft Windows. The vulnerability could allow remote code execution if a user visits a specially crafted website. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the 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.				
MS16-087	**Security Update for Windows Print Spooler Components (3170005)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker is able to execute a man-in-the-middle (MiTM) attack on a workstation or print server, or set up a rogue print server on a target network.	Critical Remote Code Execution	May require restart	3170005	Microsoft Windows
MS16-088	**Security Update for Microsoft Office (3170008)** 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
MS16-089	**Security Update for Windows Secure Kernel Mode (3170050)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure when Windows Secure Kernel Mode improperly handles objects in memory.	Important Information Disclosure	Requires restart	---	Microsoft Windows
MS16-090	**Security Update for Windows Kernel-Mode Drivers (3171481)** 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 that could exploit the vulnerabilities and take control of an affected system.	Important Elevation of Privilege	Requires restart	---	Microsoft Windows
MS16-091	**Security Update for .NET Framework (3170048)** This security update resolves a vulnerability in Microsoft .NET Framework. The vulnerability could cause information disclosure if an attacker uploads a specially	Important Information Disclosure	May require restart	---	Microsoft Windows, Microsoft .NET Framework

	crafted XML file to a web-based application.				
MS16-092	**Security Update for Windows Kernel (3171910)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow security feature bypass if the Windows kernel fails to determine how a low integrity application can use certain object manager features.	Important Security Feature Bypass	Requires restart	---	Microsoft Windows
MS16-093	**Security Update for Adobe Flash Player (3174060)** This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows RT 8.1, Windows Server 2012 R2, and Windows 10.	Critical Remote Code Execution	Requires restart	---	Microsoft Windows, Adobe Flash Player
MS16-094	**Security Update for Secure Boot (3177404)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow Secure Boot security features to be bypassed if an attacker installs an affected policy on a target device. An attacker must have either administrative privileges or physical access to install a policy and bypass Secure Boot.	Important Security Feature Bypass	Requires 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
MS16-084: Cumulative Security Update for Internet Explorer (3169991)				
CVE-2016-3204	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3240	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

CVE-2016-3241	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3242	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3243	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3245	Internet Explorer Security Feature Bypass Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3248	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3259	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3260	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3261	Internet Explorer Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3264	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3273	Microsoft Browser Information Disclosure Vulnerability	3- Exploitation Unlikely	3- Exploitation Unlikely	Not applicable
CVE-2016-3274	Microsoft Browser Spoofing Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3277	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-085: Cumulative Security Update for Microsoft Edge (3169999)				
CVE-2016-3244	Microsoft Edge Security Feature Bypass	2 - Exploitation Less Likely	4 - Not affected	Not applicable

CVE-2016-3246	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3248	Scripting Engine Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3259	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3260	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3264	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3265	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3269	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3271	Scripting Engine Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3273	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-3274	Microsoft Browser Spoofing Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3276	Microsoft Browser Spoofing Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3277	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-086: Cumulative Security Update for JScript and VBScript (3169996)				
CVE-2016-3204	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

MS16-087: Security Update for Microsoft Print Spooler (3170005)				
CVE-2016-3238	Windows Print Spooler Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3239	Windows Print Spooler Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-088: Security Update for Microsoft Office (3170008)				
CVE-2016-3278	Microsoft Office Memory Corruption Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3279	Microsoft Office Security Feature Bypass Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3280	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-3281	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3282	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3283	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-3284	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-089: Security Update for Windows Secure Kernel Mode (3170050)				
CVE-2016-3256	Windows Secure Kernel Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
MS16-090: Security Update for Windows Kernel-Mode Drivers (3171481)				
CVE-2016-3249	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-3250	Win32k Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	1 - Exploitation More Likely	Permanent

CVE-2016-3251	Win32k Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3252	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3254	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3286	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-091: Security Update for .NET Framework (3170048)				
CVE-2016-3255	.NET Information Disclosure Vulnerability	3 - Exploitation Unlikely	2 - Exploitation Less Likely	Not applicable
MS16-092: Security Update for Windows Kernel (3171910)				
CVE-2016-3258	Windows File System Security Feature Bypass	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3272	Windows Kernel Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-093: Security Update for Adobe Flash Player (3174060)				
APSB16-25	See Adobe Security Bulletin APSB16-25 for vulnerability severity and update priority ratings.	Not applicable	Not applicable	Not applicable
MS16-094: Security Update for Secure Boot (3177404)				
CVE-2016-3287	Secure Boot Security Feature Bypass	1 - Exploitation More Likely	1 - Exploitation More Likely	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	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**None**
Windows Vista Service Pack 2	Internet Explorer 9 (3170106) (Critical)	Not applicable	VBScript 5.7 (3169659) (Critical)	Windows Vista Service Pack 2 (3170455) (Critical)	Not applicable
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3170106) (Critical)	Not applicable	VBScript 5.7 (3169659) (Critical)	Windows Vista x64 Edition Service Pack 2 (3170455) (Critical)	Not applicable
Windows Server 2008					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Moderate**	**None**	**Moderate**	**Critical**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (3170106) (Moderate)	Not applicable	VBScript 5.7 (3169659) (Moderate)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3170455) (Critical)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3170106) (Moderate)	Not applicable	VBScript 5.7 (3169659) (Moderate)	Windows Server 2008 for x64-based Systems Service Pack 2 (3170455) (Critical)	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	VBScript 5.7 (3169659) (Moderate)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3170455) (Critical)	Not applicable
Windows 7					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (3170106) (Critical)	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (4038779) Security Only (Critical) Windows 7 for 32-bit Systems Service Pack 1 (4038777) Monthly Rollup (Critical)	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1	Not applicable

	(3170106) (Critical)			(4038779) Security Only (Critical) Windows 7 for x64-based Systems Service Pack 1 (4038777) Monthly Rollup (Critical)	
Windows Server 2008 R2					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 11 (3170106) (Moderate)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4038779) Security Only (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4038777) Monthly Rollup (Critical)	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 (4038779) Security Only (Critical) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4038777) Monthly Rollup (Critical)	Not applicable
Windows 8.1					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**None**
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3170106) (Critical)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (4038793) Security Only (Critical) Windows 8.1 for 32-bit Systems (4038792) Monthly Rollup (Critical)	Not applicable
Windows 8.1 for x64-based Systems	Internet Explorer 11	Not applicable	Not applicable	Windows 8.1 for x64-based Systems (4038793)	Not applicable

	(3170106) (Critical)			Security Only (Critical) Windows 8.1 for x64-based Systems (4038792) Monthly Rollup (Crfitical)	
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**None**
Windows Server 2012	Internet Explorer 10 (3170106) (Moderate)	Not applicable	Not applicable	Windows Server 2012 (4038786) Security Only (Critical) Windows Server 2012 (4038799) Monthly Rollup (Critical)	Not applicable
Windows Server 2012 R2	Internet Explorer 11 (3170106) (Moderate)	Not applicable	Not applicable	Windows Server 2012 R2 (4038793) Security Only (Critical) Windows Server 2012 R2 (4038792) Monthly Rollup (Critical)	Not applicable
Windows RT 8.1					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**None**
Windows RT 8.1	Internet Explorer 11 (3170106) (Critical)	Not applicable	Not applicable	Windows RT 8.1 (4038792) (Critical)	Not applicable
Windows 10					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Critical**	**Critical**	**None**	**Critical**	**Important**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3163912) (Critical)	Microsoft Edge (3163912) (Critical)	Not applicable	Windows 10 for 32-bit Systems (4038781) (Critical)	Windows 10 for 32-bit Systems (3163912) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (3163912) (Critical)	Microsoft Edge (3163912) (Critical)	Not applicable	Windows 10 for x64-based Systems (4038781) (Critical)	Windows 10 for x64-based Systems (3163912) (Important)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11	Microsoft Edge (3172985)	Not applicable	Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511

	(3172985) (Critical)	(Critical)		(4038783) (Critical)	for 32-bit Systems (3172985) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3172985) (Critical)	Microsoft Edge (3172985) (Critical)	Not applicable	Windows 10 Version 1511 for x64-based Systems (4038783) (Critical)	Windows 10 Version 1511 for x64-based Systems (3172985) (Important)
Windows 10 Version 1607 for 32-bit Systems	Not applicable	Not applicable	Not applicable	Windows 10 Version 1607 for 32-bit Systems (4038782) (Critical)	Not applicable
Windows 10 Version 1607 for x64-based Systems	Not applicable	Not applicable	Not applicable	Windows 10 Version 1607 for x64-based Systems (4038782) (Critical)	Not applicable
Windows Server 2016					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**Critical**	**Critical**	**None**	**Critical**	**Important**
Windows Server 2016	Not applicable	Not applicable	Not applicable	Windows Server 2016 (4038782) (Critical)	Not applicable
Server Core installation option					
Bulletin Identifier	**MS16-084**	**MS16-085**	**MS16-086**	**MS16-087**	**MS16-089**
Aggregate Severity Rating	**None**	**None**	**Moderate**	**Critical**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3169659) (Moderate)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3170455) (Critical)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3169659) (Moderate)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3170455) (Critical)	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 (3169658) (Moderate)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4038779) Security Only (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4038777) Monthly Rollup (Critical)	Not applicable

Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (4038786) Security Only (Critical) Windows Server 2012 (Server Core installation) (4038799) Monthly Rollup (Critical)	Not applicable
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (4038793) Security Only (Critical) Windows Server 2012 R2 (Server Core installation) (4038792) Monthly Rollup (Critical)	Not applicable
Windows Server 2016 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2016 (Server Core installation) (4038782) (Critical)	Not applicable

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**None**
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (3168965) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3163244) (Important) Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6 (3164025) (Important)	Not applicable	Not applicable	Not applicable
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3168965) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3163244) (Important) Microsoft .NET	Not applicable	Not applicable	Not applicable

		Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6 (3164025) (Important)			
Windows Server 2008					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3168965) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3163244) (Important) Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6 (3164025) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (3168965) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3163244) (Important) Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6 (3164025) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3168965) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3163244) (Important)	Not applicable	Not applicable	Not applicable
Windows 7					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Windows 7 for 32-bit Systems Service Pack 1 (3168965) (Important)	Microsoft .NET Framework 3.5.1 (3163245) (Important)	Not applicable	Not applicable	Not applicable

		Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164025) (Important)			
Windows 7 for x64-based Systems Service Pack 1	Windows 7 for x64-based Systems Service Pack 1 (3168965) (Important)	Microsoft .NET Framework 3.5.1 (3163245) (Important) Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164025) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**None**	**None**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3168965) (Important)	Microsoft .NET Framework 3.5.1 (3163245) (Important) Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164025) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3168965) (Important)	Microsoft .NET Framework 3.5.1 (3163245) (Important)	Not applicable	Not applicable	Not applicable
Windows 8.1					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Important**
Windows 8.1 for 32-bit	Windows 8.1 for 32-bit Systems	Microsoft .NET	Windows 8.1 for	Adobe Flash	Windows 8.1

Systems	(3168965) (Important)	Framework 3.5 (3163247) (Important) Microsoft .NET Framework 4.5.2 (3163291) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164024) (Important)	32-bit Systems (3170377) (Important) Windows 8.1 for 32-bit Systems (3169704) (Important)	Player (3174060) (Critical)	for 32-bit Systems (3172727) (Important)
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3168965) (Important)	Microsoft .NET Framework 3.5 (3163247) (Important) Microsoft .NET Framework 4.5.2 (3163291) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164024) (Important)	Windows 8.1 for x64-based Systems (3170377) (Important) Windows 8.1 for x64-based Systems (3169704) (Important)	Adobe Flash Player (3174060) (Critical)	Windows 8.1 for x64-based Systems (3172727) (Important)
Windows Server 2012 and Windows Server 2012 R2					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Moderate**	**Important**
Windows Server 2012	Windows Server 2012 (3168965) (Important)	Microsoft .NET Framework 3.5 (3163246) (Important) Microsoft .NET Framework 4.5.2 (3163250) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164023) (Important)	Windows Server 2012 (3170377) (Important) Windows Server 2012 (3169704) (Important)	Adobe Flash Player (3174060) (Moderate)	Windows Server 2012 (3172727) (Important)
Windows Server 2012 R2	Windows Server 2012 R2 (3168965) (Important)	Microsoft .NET Framework 3.5 (3163247) (Important) Microsoft .NET Framework 4.5.2 (3163291) (Important) Microsoft .NET Framework	Windows Server 2012 R2 (3170377) (Important) Windows Server 2012 R2 (3169704) (Important)	Adobe Flash Player (3174060) (Moderate)	Windows Server 2012 R2 (3172727) (Important)

		4.6/4.6.1 (3164024) (Important)			
Windows RT 8.1					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Important**
Windows RT 8.1	Windows RT 8.1 (3168965) (Important)	Microsoft .NET Framework 4.5.2 (3163291) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164024) (Important)	Windows RT 8.1 (3170377) (Important) Windows RT 8.1 (3169704) (Important)	Adobe Flash Player (3174060) (Critical)	Windows RT 8.1 (3172727) (Important)
Windows 10					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Critical**	**Important**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3163912) (Important)	Microsoft .NET Framework 3.5 (3163912) (Important) Microsoft .NET Framework 4.6 (3163912) (Important)	Windows 10 for 32-bit Systems (3163912) (Important)	Adobe Flash Player (3174060) (Critical)	Windows 10 for 32-bit Systems (3163912) (Important)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3163912) (Important)	Microsoft .NET Framework 3.5 (3163912) (Important) Microsoft .NET Framework 4.6 (3163912) (Important)	Windows 10 for x64-based Systems (3163912) (Important)	Adobe Flash Player (3174060) (Critical)	Windows 10 for x64-based Systems (3163912) (Important)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3172985) (Important)	Microsoft .NET Framework 3.5 (3172985) (Important) Microsoft .NET Framework 4.6.1 (3172985) (Important)	Windows 10 Version 1511 for 32-bit Systems (3172985) (Important)	Adobe Flash Player (3174060) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3172985) (Important)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3172985) (Important)	Microsoft .NET Framework 3.5 (3172985) (Important) Microsoft .NET	Windows 10 Version 1511 for x64-based Systems (3172985) (Important)	Adobe Flash Player (3174060) (Critical)	Windows 10 Version 1511 for x64-based Systems (3172985) (Important)

		Framework 4.6.1 (3172985) (Important)			
Windows 10 Version 1607 for 32-bit Systems	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows 10 Version 1607 for x64-based Systems	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2016					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**None**	**None**	**None**	**None**	**None**
Windows Server 2016	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Server Core installation option					
Bulletin Identifier	**MS16-090**	**MS16-091**	**MS16-092**	**MS16-093**	**MS16-094**
Aggregate Severity Rating	**Important**	**Important**	**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) (3168965) (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) (3168965) (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) (3168965) (Important)	Microsoft .NET Framework 3.5.1 (3163245) (Important) Microsoft .NET Framework 4.5.2 (3163251) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164025) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3168965) (Important)	Microsoft .NET Framework 3.5 (3163246) (Important) Microsoft .NET Framework 4.5.2 (3163250) (Important)	Windows Server 2012 (Server Core installation) (3170377) (Important) Windows Server 2012 (Server Core installation)	Not applicable	Windows Server 2012 (Server Core installation) (3172727) (Important)

		Microsoft .NET Framework 4.6/4.6.1 (3164023) (Important)	(3169704) (Important)		
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3168965) (Important)	Microsoft .NET Framework 3.5 (3163247) (Important) Microsoft .NET Framework 4.5.2 (3163291) (Important) Microsoft .NET Framework 4.6/4.6.1 (3164024) (Important)	Windows Server 2012 R2 (Server Core installation) (3170377) (Important) Windows Server 2012 R2 (Server Core installation) (3169704) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3172727) (Important)
Windows Server 2016 (Server Core installation)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Excel 2007 Service Pack 3 (3115306) (Important) Microsoft Word 2007 Service Pack 3 (3115311) (Critical)
Microsoft Office 2010	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3115315) (Critical) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3115322) (Important) Microsoft Outlook 2010 Service Pack 2 (32-bit editions) (3115246) (Important) Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions) (3115118) (Important)

	Microsoft Word 2010 Service Pack 2 (32-bit editions) (3115317) (Critical)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3115315) (Critical) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3115322) (Important) Microsoft Outlook 2010 Service Pack 2 (64-bit editions) (3115246) (Important) Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions) (3115118) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3115317) (Critical)
Microsoft Office 2013	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3115262) (Important) Microsoft Outlook 2013 Service Pack 1 (32-bit editions) (3115259) (Important) Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions) (3115254) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3115292) (Critical)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3115262) (Important) Microsoft Outlook 2013 Service Pack 1 (64-bit editions) (3115259) (Important) Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions) (3115254) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3115292) (Critical)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-088**

Aggregate Severity Rating	**Critical**
Microsoft Office 2013 RT Service Pack 1	Microsoft Excel 2013 RT Service Pack 1 (3115262) (Important) Microsoft Outlook 2013 RT Service Pack 1 (3115259) (Important) Microsoft PowerPoint 2013 RT Service Pack 1 (3115254) (Important) Microsoft Word 2013 RT Service Pack 1 (3115292) (Critical)
Microsoft Office 2016	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 (32-bit edition)	Microsoft Excel 2016 (32-bit edition) (3115272) (Important) Microsoft Outlook 2016 (32-bit edition) (3115279) (Important) Microsoft Word 2016 (32-bit edition) (3115301) (Critical)
Microsoft Office 2016 (64-bit edition)	Microsoft Excel 2016 (64-bit edition) (3115272) (Important) Microsoft Outlook 2016 (64-bit edition) (3115279) (Important) Microsoft Word 2016 (64-bit edition) (3115301) (Critical)
Microsoft Office for Mac 2011	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Critical**
Microsoft Office for Mac 2011	Microsoft Excel for Mac 2011 (3170463) (Important)
Microsoft Office for Mac 2011	Microsoft Word for Mac 2011 (3170463) (Critical)
Microsoft Office 2016 for Mac	

Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 for Mac	Microsoft Excel 2016 for Mac (3170460) (Critical)
Microsoft Office 2016 for Mac	Microsoft Word 2016 for Mac (3170460) (Critical)
Other Office Software	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Important**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3115308) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3115309) (Important)
Microsoft Excel Viewer	Microsoft Excel Viewer (3115114) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3115393) (Critical)
Microsoft Word Viewer	Microsoft Word Viewer (3115395) (Critical)

Note for MS16-088

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	**MS16-088**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Word Automation Services (3115312) (Important)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2013 Service Pack 1	Word Automation Services (3115285)

	(Important)
Microsoft SharePoint Server 2016	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2016	Microsoft SharePoint Server 2016 (3115299) (Important)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3115318) (Important)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3115289) (Important)
Office Online Server	
Bulletin Identifier	**MS16-088**
Aggregate Severity Rating	**Important**
Office Online Server	Office Online Server (3115386) (Important)

Note for MS16-088

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

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 (July 12, 2016): Bulletin Summary published.
- V1.1 (July 29, 2016): For MS16-087, added a Known Issues reference to the Executive Summaries table. If you are using network printing in your environment, after you apply the 3170005 security update you may receive a warning about installing a printer driver, or the driver may fail to install without notification. For more information about the update and the known issue, see Microsoft Knowledge Base Article 3170005.
- V1.2 (March 17, 2017) For MS16-084, removed CVE-2016-3276 from the Exploitability Index because Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 are not affected. This is an informational change only.
- V2.0: (September 12, 2017): For MS16-087, to address known issues with the 3170455 update for CVE-2016-3238, Microsoft has made available the following updates for currently-supported versions of Microsoft Windows:
    - Rereleased update 3170455 for Windows Server 2008
    - Monthly Rollup 4038777 and Security Update 4038779 for Windows 7 and Windows Server 2008 R2
    - Monthly Rollup 4038799 and Security Update 4038786 for Windows Server 2012
    - Monthly Rollup 4038792 and Security Update 4038793 for Windows 8.1 and Windows Server 2012 R2
    - Cumulative Update 4038781 for Windows 10
    - Cumulative Update 4038781 for Windows 10 Version 1511
    - Cumulative Update 4038782 for Windows 10 Version 1607 and Windows Server 2016.

  Microsoft recommends that customers running Windows Server 2008 reinstall update 3170455. Microsoft recommends that customers running other supported versions of Windows install the appropriate update. See Microsoft Knowledge Base Article 3170005 for more information

Page generated 2017-09-08 13:03-07:00.