Microsoft Security Bulletin Summary for August 2016

Published: August 9, 2016 | Updated: September 12, 2017

Version: 3.0

This bulletin summary lists security bulletins released for August 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
MS16-095	**Cumulative Security Update for Internet Explorer (3177356)** 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	3176492 3176493 3176495	Microsoft Windows, Internet Explorer
MS16-096	**Cumulative Security Update for Microsoft Edge (3177358)** 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	3176492 3176493 3176495	Microsoft Windows, Microsoft Edge

MS16-097	**Security Update for Microsoft Graphics Component (3177393)** This security update resolves vulnerabilities in Microsoft Windows, Microsoft Office, Skype for Business, and Microsoft Lync. The vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical Remote Code Execution	May require restart	3176492 3176493 3176495	Microsoft Windows, Microsoft Office, Microsoft Communications Platforms and Software
MS16-098	**Security Update for Windows Kernel-Mode Drivers (3178466)** This security update resolves vulnerabilities in Microsoft Windows. 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	3176492 3176493 3176495 3177725	Microsoft Windows
MS16-099	**Security Update for Microsoft Office (3177451)** 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
MS16-100	**Security Update for Secure Boot (3179577)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker installs an affected boot manager and bypasses Windows security features.	Important Security Feature Bypass	Does not require restart	3179577	Microsoft Windows
MS16-101	**Security Update for Windows Authentication Methods (3178465)** This security update resolves multiple vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker runs a specially crafted application on a domain-joined system.	Important Elevation of Privilege	Requires restart	3176492 3176493 3176495 3167679	Microsoft Windows
MS16-102	**Security Update for Microsoft Windows PDF Library (3182248)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user views specially crafted PDF content online or opens a specially crafted PDF document. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user	Critical Remote Code Execution	May require restart	3176492 3176493	Microsoft Windows

	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.				
MS16-103	**Security Update for ActiveSyncProvider (3182332)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure when Universal Outlook fails to establish a secure connection.	Important Information Disclosure	Requires restart	3176492 3176493	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
MS16-095: Cumulative Security Update for Internet Explorer (3177356)				
CVE-2016-3288	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3289	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3290	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3293	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3321	Internet Explorer Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3322	Microsoft Browser Memory	1 - Exploitation More Likely	4 - Not affected	Not applicable

	Corruption Vulnerability			
CVE-2016-3326	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3327	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3329	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-096: Cumulative Security Update for Microsoft Edge (3177358)				
CVE-2016-3289	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3293	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3296	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3319	Microsoft PDF Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3322	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-3326	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2016-3327	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3329	Microsoft Browser Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
MS16-097: Security Update for Microsoft Graphics Component (3177393)				
CVE-2016-3301	Windows Graphics Component RCE Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

CVE-2016-3303	Windows Graphics Component RCE Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-3304	Windows Graphics Component RCE Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466)				
CVE-2016-3308	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3309	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3310	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3311	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-099: Security Update for Microsoft Office (3177451)				
CVE-2016-3313	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3315	Microsoft OneNote Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-3316	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-3317	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-3318	Graphics Component Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS16-100: Security Update for Secure Boot (3179577)				
CVE-2016-3320	Secure Boot Security Feature Bypass Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-101: Security Update for Windows Authentication Methods (3178465)				

CVE-2016-3237	Kerberos Security Feature Bypass Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-3300	NetLogon Elevation of Privilege Vulnerability	4 - Not applicable	2 - Exploitation Less Likely	Not applicable
MS16-102: Security Update for Microsoft Windows PDF Library (3182248)				
CVE-2016-3319	Microsoft PDF Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-103: Security Update for ActiveSyncProvider (3182332)				
CVE-2016-3312	Universal Outlook Information Disclosure Vulnerability	3 - Exploitation Unlikely	4 - Not affected	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	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (3175443) (Critical)	Not applicable	Windows Vista Service Pack 2 (3178034) (Critical)	Windows Vista Service Pack 2 (3177725) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3175443) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3178034) (Critical)	Windows Vista x64 Edition Service Pack 2 (3177725) (Important)
Windows Server 2008				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Important**
Windows Server 2008 for	Internet Explorer 9	Not applicable	Windows Server 2008	Windows Server 2008

32-bit Systems Service Pack 2	(3175443) (Moderate)		for 32-bit Systems Service Pack 2 (3178034) (Critical)	for 32-bit Systems Service Pack 2 (3177725) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3175443) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3178034) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (3177725) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3178034) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3177725) (Important)
Windows 7				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (4021558) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3178034) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3177725) (Important)
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (4021558) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3178034) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3177725) (Important)
Windows Server 2008 R2				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 11 (4021558) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3178034) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3177725) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3178034) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3177725) (Important)
Windows 8.1				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Important**
Windows 8.1 for 32-bit	Internet Explorer 11	Not applicable	Windows 8.1 for 32-	Windows 8.1 for 32-

Systems	(4021558) (Critical)		bit Systems (3178034) (Critical)	bit Systems (3177725) (Important)
Windows 8.1 for x64-based Systems	Internet Explorer 11 (4021558) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3178034) (Critical)	Windows 8.1 for x64-based Systems (3177725) (Important)
Windows Server 2012 and Windows Server 2012 R2				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Important**
Windows Server 2012	Internet Explorer 10 (4021558) (Moderate)	Not applicable	Windows Server 2012 (3178034) (Critical)	Windows Server 2012 (3177725) (Important)
Windows Server 2012 R2	Internet Explorer 11 (4021558) (Moderate)	Not applicable	Windows Server 2012 R2 (3178034) (Critical)	Windows Server 2012 R2 (3177725) (Important)
Windows RT 8.1				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Important**
Windows RT 8.1	Internet Explorer 11 (4021558) (Critical)	Not applicable	Windows RT 8.1 (3178034) (Critical)	Windows RT 8.1 (3177725) (Important)
Windows 10				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Important**
Windows 10 for 32-bit Systems	Internet Explorer 11 (4022727) (Critical)	Microsoft Edge (3176492) (Critical)	Windows 10 for 32-bit Systems (3176492) (Critical)	Windows 10 for 32-bit Systems (3176492) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (4022727) (Critical)	Microsoft Edge (3176492) (Critical)	Windows 10 for x64-based Systems (3176492) (Critical)	Windows 10 for x64-based Systems (3176492) (Important)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (4022714) (Critical)	Microsoft Edge (3176493) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3176493) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3176493) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (4022714) (Critical)	Microsoft Edge (3176493) (Critical)	Windows 10 Version 1511 for x64-based Systems (3176493) (Critical)	Windows 10 Version 1511 for x64-based Systems (3176493) (Important)
Windows 10 Version 1607 for 32-bit Systems	Internet Explorer 11 (4022715)	Microsoft Edge (3176495)	Windows 10 Version 1607 for 32-bit	Windows 10 Version 1607 for 32-bit

	(Critical)	(Critical)	Systems (3176495) (Critical)	Systems (3176495) (Important)
Windows 10 Version 1607 for x64-based Systems	Internet Explorer 11 (4022715) (Critical)	Microsoft Edge (3176495) (Critical)	Windows 10 Version 1607 for x64-based Systems (3176495) (Critical)	Windows 10 Version 1607 for x64-based Systems (3176495) (Important)
Windows 10 Version 1703 for 32-bit Systems	Internet Explorer 11 (4038788) (Critical)	Not applicable	Not applicable	Not applicable
Windows 10 Version 1703 for x64-based Systems	Internet Explorer 11 (4038788) (Critical)	Not applicable	Not applicable	Not applicable
Server Core installation option				
Bulletin Identifier	**MS16-095**	**MS16-096**	**MS16-097**	**MS16-098**
Aggregate Severity Rating	**None**	**None**	**Critical**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3178034) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3170455) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3178034) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3170455) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3178034) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3170455) (Important)
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3178034) (Critical)	Windows Server 2012 (Server Core installation) (3170455) (Important)
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3178034) (Critical)	Windows Server 2012 R2 (Server Core installation) (3170455) (Important)

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**
Windows Vista Service Pack 2	Not applicable	Windows Vista Service Pack 2 (3167679) (Important)	Not applicable	Not applicable
Windows Vista x64 Edition Service Pack 2	Not applicable	Windows Vista x64 Edition Service Pack 2 (3167679) (Important)	Not applicable	Not applicable
Windows Server 2008				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3167679) (Important)	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3167679) (Important)	Not applicable	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3167679) (Important)	Not applicable	Not applicable
Windows 7				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3167679) (Important)	Not applicable	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3167679) (Important)	Not applicable	Not applicable
Windows Server 2008 R2				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**None**	**Important**	**None**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3167679) (Important)	Not applicable	Not applicable
Windows Server 2008 R2 for	Not applicable	Windows Server 2008 R2 for Itanium-	Not applicable	Not applicable

Itanium-based Systems Service Pack 1		based Systems Service Pack 1 (3167679) (Important)		
Windows 8.1				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**Important**	**Important**	**Critical**	**None**
Windows 8.1 for 32-bit Systems	Windows 8.1 for 32-bit Systems (3172729) (Important)	Windows 8.1 for 32-bit Systems (3167679) (Important) Windows 8.1 for 32-bit Systems (3177108) (Important)	Windows 8.1 for 32-bit Systems (3175887) (Critical)	Not applicable
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3172729) (Important)	Windows 8.1 for x64-based Systems (3167679) (Important) Windows 8.1 for x64-based Systems (3177108) (Important)	Windows 8.1 for x64-based Systems (3175887) (Critical)	Not applicable
Windows Server 2012 and Windows Server 2012 R2				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**Important**	**Important**	**Critical**	**None**
Windows Server 2012	Windows Server 2012 (3172729) (Important)	Windows Server 2012 (3177108) (Important)	Windows Server 2012 (3175887) (Critical)	Not applicable
Windows Server 2012 R2	Windows Server 2012 R2 (3172729) (Important)	Windows Server 2012 R2 (3167679) (Important) Windows Server 2012 R2 (3177108) (Important)	Windows Server 2012 R2 (3175887) (Critical)	Not applicable
Windows RT 8.1				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**Important**	**Important**	**Critical**	**None**
Windows RT 8.1	Windows RT 8.1 (3172729) (Important)	Windows RT 8.1 (3167679) (Important) Windows RT 8.1 (3177108) (Important)	Windows RT 8.1 (3175887) (Critical)	Not applicable
Windows 10				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**Important**	**Important**	**Critical**	**Important**

Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3172729) (Important)	Windows 10 for 32-bit Systems (3176492) (Important)	Windows 10 for 32-bit Systems (3176492) (Critical)	Windows 10 for 32-bit Systems (3176492) (Important)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3172729) (Important)	Windows 10 for x64-based Systems (3176492) (Important)	Windows 10 for x64-based Systems (3176492) (Critical)	Windows 10 for x64-based Systems (3176492) (Important)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3172729) (Important)	Windows 10 Version 1511 for 32-bit Systems (3176493) (Important)	Windows 10 Version 1511 for 32-bit Systems (3176493) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3176493) (Important)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3172729) (Important)	Windows 10 Version 1511 for x64-based Systems (3176493) (Important)	Windows 10 Version 1511 for x64-based Systems (3176493) (Critical)	Windows 10 Version 1511 for x64-based Systems (3176493) (Important)
Windows 10 Version 1607 for 32-bit Systems	Not applicable	Windows 10 Version 1607 for 32-bit Systems (3176495) (Important)	Not applicable	Not applicable
Windows 10 Version 1607 for x64-based Systems	Not applicable	Windows 10 Version 1607 for x64-based Systems (3176495) (Important)	Not applicable	Not applicable
Server Core installation option				
Bulletin Identifier	**MS16-100**	**MS16-101**	**MS16-102**	**MS16-103**
Aggregate Severity Rating	**Important**	**Important**	**Critical**	**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) (3167679) (Important)	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) (3167679) (Important)	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) (3167679) (Important)	Not applicable	Not applicable
Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3172729) (Important)	Windows Server 2012 (Server Core installation) (3177108) (Important)	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server	Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable

	Core installation) (3172729) (Important)	(3167679) (Important) Windows Server 2012 R2 (Server Core installation) (3177108) (Important)		

Microsoft Office Suites and Software

Microsoft Office 2007		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**Critical**	**Important**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (3115109) (Critical)	Microsoft Office 2007 Service Pack 3 (3114442) (Important) Microsoft Office 2007 Service Pack 3 (3114893) (Important) Microsoft OneNote 2007 Service Pack 3 (3114456) (Important) Microsoft Word 2007 Service Pack 3 (3115465) (Important)
Microsoft Office 2010		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**Critical**	**Important**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3115131) (Critical)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114400) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114869) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3115468) (Important) Microsoft OneNote 2010 Service Pack 2 (32-bit editions) (3114885) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3115471) (Important)

Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3115131) (Critical)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114400) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114869) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3115468) (Important) Microsoft OneNote 2010 Service Pack 2 (64-bit editions) (3114885) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3115471) (Important)
Microsoft Office 2013		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Not applicable	Microsoft Office 2013 Service Pack 1 (32-bit editions) (3114340) (Important) Microsoft Office 2013 Service Pack 1 (32-bit editions) (3115427) (Important) Microsoft OneNote 2013 Service Pack 1 (32-bit editions) (3115256) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3115449) (Critical)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Not applicable	Microsoft Office 2013 Service Pack 1 (64-bit editions) (3114340) (Important) Microsoft Office 2013 Service Pack 1 (64-bit editions) (3115427) (Important) Microsoft OneNote 2013 Service Pack 1 (64-bit editions) (3115256) (Important)

		Microsoft Word 2013 Service Pack 1 (64-bit editions) (3115449) (Critical)
Microsoft Office 2013 RT		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2013 RT Service Pack 1	Not applicable	Microsoft Office 2013 RT Service Pack 1 (3114340) (Important) Microsoft Office 2013 RT Service Pack 1 (3115427) (Important) Microsoft OneNote 2013 RT Service Pack 1 (3115256) (Important) Microsoft Word 2013 RT Service Pack 1 (3115449) (Critical)
Microsoft Office 2016		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2016 (32-bit edition)	Not applicable	Microsoft Office 2016 (32-bit edition) (3115415) (Important) Microsoft OneNote 2016 (32-bit edition) (3115419) (Important) Microsoft Word 2016 (32-bit edition) (3115439) (Critical)
Microsoft Office 2016 (64-bit edition)	Not applicable	Microsoft Office 2016 (64-bit edition) (3115415) (Important) Microsoft OneNote 2016 (64-bit edition) (3115419) (Important) Microsoft Word 2016 (64-bit edition) (3115439) (Critical)
Microsoft Office for Mac 2011		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office for Mac 2011	Not applicable	Microsoft Word for Mac 2011

		(3179162) (Important)
Microsoft Office 2016 for Mac		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office 2016 for Mac	Not applicable	Microsoft OneNote 2016 for Mac (3179163) (Important) Microsoft Word 2016 for Mac (3179163) (Important)
Other Office Software		
Bulletin Identifier	**MS16-097**	**MS16-099**
Aggregate Severity Rating	**Critical**	**Important**
Microsoft Word Viewer	Microsoft Word Viewer (3115481) (Critical)	Microsoft Word Viewer (3115479) (Important) Microsoft Word Viewer (3115480) (Important)

Note for MS16-097

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

Microsoft Communications Platforms and Software

Skype for Business 2016	
Bulletin Identifier	**MS16-097**
Aggregate Severity Rating	**Critical**
Skype for Business 2016 (32-bit editions)	Skype for Business 2016 (32-bit editions) (3115408) (Critical)
Skype for Business Basic 2016 (32-bit editions)	Skype for Business Basic 2016 (32-bit editions) (3115408) (Critical)
Skype for Business 2016 (64-bit editions)	Skype for Business 2016 (64-bit editions) (3115408) (Critical)
Skype for Business Basic 2016 (64-bit editions)	Skype for Business Basic 2016 (64-bit editions) (3115408) (Critical)
Microsoft Lync 2013	

Bulletin Identifier	**MS16-097**
Aggregate Severity Rating	**Critical**
Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business) (3115431) (Critical)
Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic) (3115431) (Critical)
Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business) (3115431) (Critical)
Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic) (3115431) (Critical)
Microsoft Lync 2010	
Bulletin Identifier	**MS16-097**
Aggregate Severity Rating	**Critical**
Microsoft Lync 2010 (32-bit)	Microsoft Lync 2010 (32-bit) (3174301) (Critical)
Microsoft Lync 2010 (64-bit)	Microsoft Lync 2010 (64-bit) (3174301) (Critical)
Microsoft Lync 2010 Attendee (user level install)	Microsoft Lync 2010 Attendee (user level install) (3174302) (Critical)
Microsoft Lync 2010 Attendee (admin level install)	Microsoft Lync 2010 Attendee (admin level install) (3174304) (Critical)
Microsoft Live Meeting 2007 Console	
Bulletin Identifier	**MS16-097**
Aggregate Severity Rating	**Critical**
Microsoft Live Meeting 2007 Console	Microsoft Live Meeting 2007 Console (3174305) (Critical)

Note for MS16-097

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

Detection and Deployment Tools and Guidance

Several resources are available to help administrators deploy security updates.

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

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

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

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

Acknowledgments

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

Other Information

Microsoft Windows Malicious Software Removal Tool

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

Non-Security Updates on MU, WU, and WSUS

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

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

Microsoft Active Protections Program (MAPP)

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

Security Strategies and Community

Update Management Strategies

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

Obtaining Other Security Updates

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

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

IT Pro Security Community

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

Support

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

Security solutions for IT professionals: TechNet Security Troubleshooting and Support

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

Local support according to your country: International Support

Disclaimer

Revisions

- V1.0 (August 9, 2016): Bulletin Summary published.
- V1.1 (August 10, 2016): For MS16-101, Bulletin Summary revised to correct the security impact for CVE-2016-3237 from elevation of privilege to security feature bypass. This is an informational change only. Customers who have already successfully installed the update do not need to take any action.
- V1.2 (August 11, 2016): For MS16-102, Bulletin Summary revised to remove Windows Server 2012 R2 (Server Core installation) from the affected software table because the Server Core version of Windows Server 2012 R2 is not affected. These are informational changes only. Customers who have already successfully installed the update do not need to take any action.
- V1.3 (August 12, 2016): For MS16-102, Bulletin Summary revised to remove Windows 10 version 1607 from the affected software table because it is not affected. This is an informational change only. Customers who have already successfully installed the update do not need to take any action.
- V1.4 (August 18, 2016): For MS16-095, MS16-096, MS16-097, MS16-098, MS16-101, MS16-102, and MS16-103, Bulletin Summary revised to add Known Issues references to the Executive Summaries table. See the relevant Knowledge Base articles for more information.
- V2.0 (June 13, 2017): To comprehensively address CVE-2016-3326, Microsoft is releasing June security updates for all affected Microsoft browsers. Microsoft recommends that customers running affected Microsoft browsers should install the applicable June security update to be fully protected from this vulnerability. See the applicable Release Notes or Microsoft Knowledge Base article for more information.
- V3.0 (September 12, 2017): For MS16-095, revised the Windows Operating System and Components Affected Software table to include Internet Explorer 11 installed on Windows 10 Version 1703 for 32-bit Systems and Internet Explorer 11 installed on Windows 10 Version 1703 for x64-based Systems because they are affected by CVE-2016-3326. Microsoft recommends that customers running Internet Explorer on Windows 10 Version 1703 install update 4038788 to be protected from this vulnerability.

Page generated 2017-09-05 09:23-07:00.