Microsoft Security Bulletin MS17-010 - Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

On this page

Affected Software and Vulnerability Severity Ratings

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see Microsoft Support Lifecycle.

The severity ratings indicated for each affected software assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the March bulletin summary.

Note Please see the Security Update Guide for a new approach to consuming the security update information. You can customize your views and create affected software spreadsheets, as well as download data via a restful API. For more information, please see the Security Updates Guide FAQ. As a reminder, the Security Updates Guide will be replacing security bulletins. Please see our blog post, Furthering our commitment to security updates, for more details.

Operating System	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146	Windows SMB Information Disclosure Vulnerability – CVE-2017-0147	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148	Updates Replaced
Windows Vista							
Windows Vista Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows Vista x64 Edition	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114

Service Pack 2 (4012598)							
Windows Server 2008							
Windows Server 2008 for 32-bit Systems Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows Server 2008 for x64-based Systems Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows 7							
Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for 32-bit Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows 7 for x64-based Systems Service Pack 1 (4012212)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None

Security Only[1]							
Windows 7 for x64-based Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows Server 2008 R2							
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows 8.1							

Windows 8.1 for 32-bit Systems (4012213) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 8.1 for 32-bit Systems (4012216) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3205401
Windows 8.1 for x64-based Systems (4012213) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 8.1 for x64-based Systems (4012216) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3205401
Windows Server 2012 and Windows Server 2012 R2							
Windows Server 2012 (4012214) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows Server 2012 (4012217) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3205409
Windows Server 2012 R2 (4012213) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows Server 2012 R2 (4012216) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3205401

Windows RT 8.1							
Windows RT 8.1[2] (4012216) Monthly Rollup	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3205401
Windows 10							
Windows 10 for 32-bit Systems [3] (4012606)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210720
Windows 10 for x64-based Systems [3] (4012606)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210720
Windows 10 Version 1511 for 32-bit Systems [3] (4013198)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210721
Windows 10 Version 1511 for x64-based Systems [3] (4013198)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210721
Windows 10 Version 1607 for 32-bit Systems [3] (4013429)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3213986
Windows 10 Version 1607 for x64-based Systems [3] (4013429)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3213986
Windows Server 2016							
Windows Server 2016 for x64-based Systems [3] (4013429)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3213986
Server Core installation option							

Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows Server 2012 (Server Core installation) (4012214) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows	**Critical**	**Critical**	**Critical**	**Critical**	**Important**	**Critical**	3205409

Server 2012 (Server Core installation) (4012217) Monthly Rollup[1]	Remote Code Execution	Remote Code Execution	Remote Code Execution	Remote Code Execution	Information Disclosure	Remote Code Execution	
Windows Server 2012 R2 (Server Core installation) (4012213) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows Server 2012 R2 (Server Core installation) (4012216) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3205401
Windows Server 2016 for x64-based Systems [3] (Server Core installation) (4013429)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3213986

[1]Beginning with the October 2016 release, Microsoft has changed the update servicing model for Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2. For more information, please see this Microsoft TechNet article.

[2]This update is only available via Windows Update.

[3] Windows 10 and Windows Server 2016 updates are cumulative. The monthly security release includes all security fixes for vulnerabilities that affect Windows 10, in addition to non-security updates. The updates are available via the Microsoft Update Catalog. Please note that effective December 13, 2016, Windows 10 and Windows Server 2016 details for the Cumulative Updates will be documented in Release Notes. Please refer to the Release Notes for OS Build numbers, Known Issues, and affected file list information.

*The Updates Replaced column shows only the latest update in any chain of superseded updates. For a comprehensive list of updates replaced, go to the Microsoft Update Catalog, search for the update KB number, and then view update details (updates replaced information is provided on the Package Details tab).

Vulnerability Information

Multiple Windows SMB Remote Code Execution Vulnerabilities

Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.

To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

The security update addresses the vulnerabilities by correcting how SMBv1 handles these specially crafted requests.

The following table contains links to the standard entry for each vulnerability in the Common Vulnerabilities and Exposures list:

Vulnerability title	CVE number	Publicly disclosed	Exploited
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0143	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0144	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0145	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0146	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0148	No	No

Mitigating Factors

Microsoft has not identified any mitigating factors for these vulnerabilities.

Workarounds

The following workarounds may be helpful in your situation:

- **Disable SMBv1**
  For customers running Windows Vista and later

  See Microsoft Knowledge Base Article 2696547.

  Alternative method for customers running Windows 8.1 or Windows Server 2012 R2 and later

  For client operating systems:

  1. Open **Control Panel**, click **Programs**, and then click **Turn Windows features on or off.**
  2. In the Windows Features window, clear the **SMB1.0/CIFS File Sharing Support** checkbox, and then click **OK** to close the window.
  3. Restart the system.

  For server operating systems:

  1. Open **Server Manager** and then click the **Manage** menu and select **Remove Roles and Features**.
  2. In the Features window, clear the **SMB1.0/CIFS File Sharing Support** check box, and then click **OK** to close the window.
  3. Restart the system.

  Impact of workaround. The SMBv1 protocol will be disabled on the target system.

  How to undo the workaround. Retrace the workaround steps, and select the **SMB1.0/CIFS File Sharing Support** check box to restore the SMB1.0/CIFS File Sharing Support feature to an active state.

Windows SMB Information Disclosure Vulnerability – CVE-2017-0147

An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server.

To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

The following table contains links to the standard entry for each vulnerability in the Common Vulnerabilities and Exposures list:

Vulnerability title	CVE number	Publicly disclosed	Exploited
Windows SMB Information Disclosure Vulnerability	CVE-2017-0147	No	No

Mitigating Factors

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

The following workarounds may be helpful in your situation:

- **Disable SMBv1**
  For customers running Windows Vista and later

  See Microsoft Knowledge Base Article 2696547.

  Alternative method for customers running Windows 8.1 or Windows Server 2012 R2 and later

  For client operating systems:

  1. Open **Control Panel**, click **Programs**, and then click **Turn Windows features on or off.**
  2. In the Windows Features window, clear the **SMB1.0/CIFS File Sharing Support** checkbox, and then click **OK** to close the window.
  3. Restart the system.

  For server operating systems:

  1. Open **Server Manager** and then click the **Manage** menu and select **Remove Roles and Features**.
  2. In the Features window, clear the **SMB1.0/CIFS File Sharing Support** check box, and then click **OK** to close the window.
  3. Restart the system.

  Impact of workaround. The SMBv1 protocol will be disabled on the target system.

  How to undo the workaround. Retrace the workaround steps, and select the **SMB1.0/CIFS File Sharing Support** check box to restore the SMB1.0/CIFS File Sharing Support feature to an active state.

Security Update Deployment

For Security Update Deployment information, see the Microsoft Knowledge Base article referenced here in the Executive Summary.

Acknowledgments

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

Disclaimer

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 (March 14, 2017): Bulletin published.

Page generated 2017-05-08 07:15-07:00.