Microsoft Security Bulletin MS08-067 – Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

Top of section

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040

Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None
Windows XP Professional x64 Edition	Remote Code Execution	Critical	MS06-040
Windows XP Professional x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 Service Pack 1	Remote Code Execution	Critical	MS06-040
Windows Server 2003 Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 x64 Edition	Remote Code Execution	Critical	MS06-040
Windows Server 2003 x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 with SP1 for Itanium-based Systems	Remote Code Execution	Critical	MS06-040
Windows Server 2003 with SP2 for Itanium-based Systems	Remote Code Execution	Critical	None
Windows Vista and Windows Vista Service Pack 1	Remote Code Execution	Important	None
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	Remote Code Execution	Important	None
Windows Server 2008 for 32-bit Systems*	Remote Code Execution	Important	None
Windows Server 2008 for x64-based Systems*	Remote Code Execution	Important	None
Windows Server 2008 for Itanium-based Systems	Remote Code Execution	Important	None

***Windows Server 2008 server core installation affected.** For supported editions of Windows Server 2008, this update applies, with the same severity rating, whether or not Windows Server 2008 was installed using the Server Core installation option. For more information on this installation option, see Server Core. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see Compare Server Core Installation Options.

Top of section

Frequently Asked Questions (FAQ) Related to This Security Update

Vulnerability Information

Severity Ratings and Vulnerability Identifiers

Server Service Vulnerability - CVE-2008-4250

Update Information

Detection and Deployment Tools and Guidance

Security Update Deployment

Other Information

Support

- Customers in the U.S. and Canada can receive technical support from Microsoft Product Support Services at 1-866-PCSAFETY. There is no charge for support calls that are associated with security updates.
- International customers can receive support from their local Microsoft subsidiaries. There is no charge for support that is associated with security updates. For more information about how to contact Microsoft for support issues, visit the International Support Web site.

Top of section

Disclaimer

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

Top of section

Revisions

- V1.0 (October 23, 2008): Bulletin published.

Top of section

Top of page