



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Critical Infrastructure Information Notice- CIIN-08-297-01

October 23, 2008

Vulnerability in Microsoft Server Service Could Allow Remote Code Execution

Overview

Microsoft released an out-of-band Security Bulletin, [MS08-067](#), to address a vulnerability in Microsoft Server Service. This vulnerability may allow a remote attacker to execute arbitrary code on an affected system by sending a specially crafted RPC request. Microsoft is aware of limited active exploitation of this vulnerability. Microsoft expects an exploit to be weaponized soon after public release.

US-CERT is issuing this notice to warn organizations of this vulnerability and provide mitigation strategies to prevent further compromises from occurring.

Technical Details

This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code on Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems. According to Microsoft, Windows Vista and Windows Server 2008 systems require that the attacker be authenticated. It is possible that this vulnerability could be used to create a self-propagating malicious application.

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. The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests.

According to Microsoft, the following table shows the vulnerability severity ratings and maximum security impact by affected software:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Vulnerability Severity Rating and Maximum Security Impact by Affected Software		
Affected Software	Server Service Vulnerability - CVE-2008-4250	Aggregate Severity Rating
Microsoft Windows 2000 Service Pack 4	Critical Remote Code Execution	Critical
Windows XP Service Pack 2 and Windows XP Service Pack 3	Critical Remote Code Execution	Critical
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2	Critical Remote Code Execution	Critical
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2	Critical Remote Code Execution	Critical
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2	Critical Remote Code Execution	Critical
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems	Critical Remote Code Execution	Critical
Windows Vista and Windows Vista Service Pack 1	Important Remote Code Execution	Important
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	Important Remote Code Execution	Important
Windows Server 2008 for 32-bit Systems*	Important Remote Code Execution	Important
Windows Server 2008 for x64-based Systems*	Important Remote Code Execution	Important
Windows Server 2008 for Itanium-based Systems	Important Remote Code Execution	Important

***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](#).

US-CERT will continue to monitor this activity and provide additional information as necessary.

Recommendations

Organizations must review Microsoft Security Bulletin [MS08-067](#) and apply the patch to vulnerable systems as soon as possible. If the patch cannot be applied immediately, US-CERT recommends that organizations consider following the workarounds and mitigation strategies provided by Microsoft:

- Disable the Server and Computer Browser services.
- On Windows Vista and Windows Server 2008, filter the affected RPC identifier.
- Ensure organizations have blocked TCP ports 139 and 445 at the firewall.
- To help protect from network-based attempts to exploit this vulnerability, use a personal firewall, such as the Internet Connection Firewall.

More details regarding the way in which to implement the above workarounds are available in the security bulletin.

NOTE: US-CERT reminds agencies that proper impact analysis should be performed prior to taking defensive measures.

Additionally, Microsoft states that “firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.”

US-CERT also recommends that agencies review the following documents:

- [Technical Cyber Security Alert TA08-297A](#) – Microsoft Windows Server Service RPC Vulnerability
- [Vulnerability Note VU#827267](#) – Microsoft Server Service RPC stack buffer overflow vulnerability

Organizations should follow their established internal procedures if any suspected malicious activity is observed, and report their findings to US-CERT for correlation against other incidents.

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov

Voice: 1-888-282-0870

Incident Reporting Form: <https://forms.us-cert.gov/report/>

Document FAQ

UNCLASSIFIED//FOR OFFICIAL USE ONLY

What is a CIIN? A Critical Infrastructure Information Notice (CIIN) is intended to provide warning to US critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks.

I see that this document is labeled as UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). Can I distribute this to other people? Per the U//FOUO warning, this document may be shared with personnel who have a valid “need to know.” With the case of a CIIN, this is defined as a person or group that has a direct role in securing US critical infrastructure networks. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

UNCLASSIFIED//FOR OFFICIAL USE ONLY