

## Cisco Security Agent and Microsoft Vulnerability MS08-067 Vulnerability in Server Service Could Allow Remote Code Execution

PB514332

### Summary

A critical vulnerability has been discovered in the Remote Procedure Call (RPC) server service in Microsoft Windows 2000, 2003, XP, Vista, and 2008 operating systems. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request.

This vulnerability has already been exploited in several attacks. Cisco has obtained exploit files, and has confirmed that the Cisco<sup>®</sup> Security Agent Versions 5.2 and 6.0 are effective in stopping these exploits, using the default security policy configuration.

### Details of the Vulnerability

Details of the vulnerability are documented by Microsoft [1] and by the Computer Emergency Response Team (CERT) [2]:

A remote code execution vulnerability exists in the Server service on Windows systems. The vulnerability is due to the service not properly handling specially crafted RPC requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability over RPC without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. If successfully exploited, an attacker could then install programs or view, change, or delete data, or create new accounts with full user rights.

RPC is a protocol that a program can use to request a service from a program located on another computer in a network. RPC helps with interoperability because the program using RPC does not have to understand the network protocols that are supporting communication. In RPC, the requesting program is the client and the service-providing program is the server.

### How Cisco Security Agent Stops the Exploit

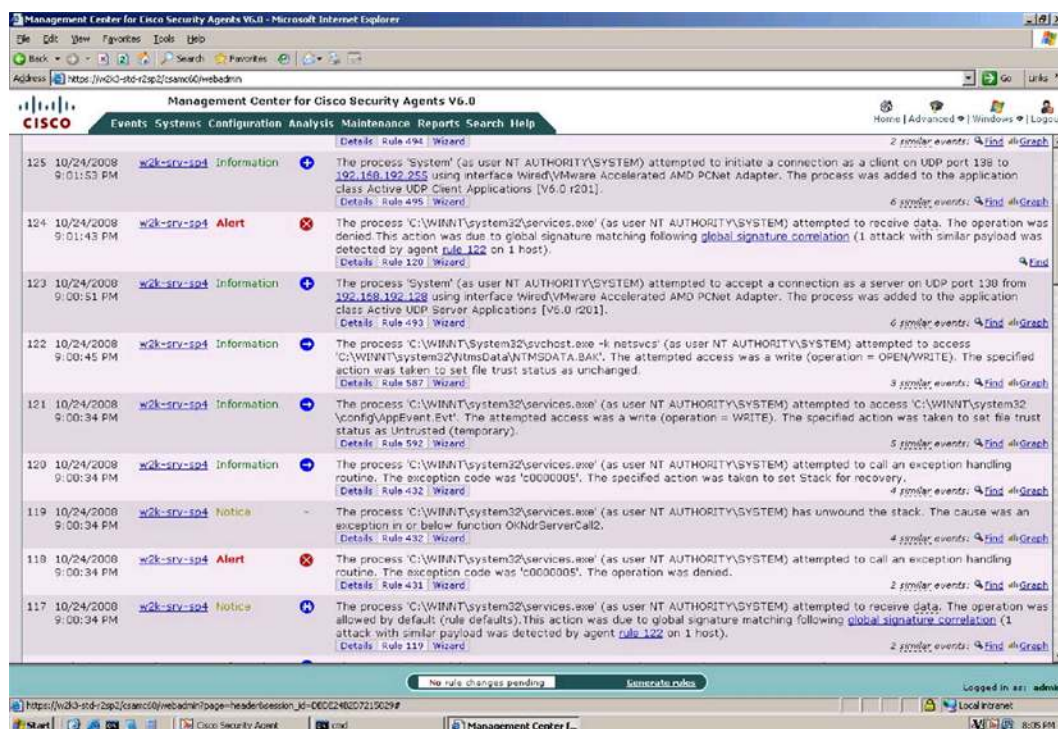
Cisco Security Agent default policies contain multiple rules that stop the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection.

Cisco Security Agent helps protect against attempts to exploit this vulnerability through use of the Network Access Control rule that prevents the endpoint from attempting to act as a server for network services and accepting SMB null sessions. This closes the possibility of unauthenticated exploitation (for example, via a worm). This is the default configuration; no action is required by Cisco Security Agent customers.

Cisco Security Agent Version 6.0 extends this protection by automatically creating a custom buffer overflow signature for code exploiting MS08-067. Agents automatically create signatures for these exploits, and install them after seeing subsequent attacks that match the signature. This eliminates the possibility of exploitation from authenticated sources (e.g., by remote systems offering login credentials, rather than unauthenticated connections via null session). This is the default configuration; no action is required by Cisco Security Agent customers.

This testing is shown in Figure 1.

**Figure 1.** Cisco Security Agent Default Configuration Stops the MS08-067 Exploit (Tested on Cisco Security Agent 6.0)



**Note:** The exploit was tested at Cisco, with the agent in Audit mode, which will cause the agent to alert (but not block) malicious behavior. This was done to observe all possible ways that the Cisco Security Agent default policies would stop the exploit. When the agent is in Protect mode (the typical operational configuration), the first rule would kill the exploit: no subsequent events would be seen, since the exploit would be terminated before it could perform any malicious actions.

Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for Cisco Security Agents to be effective. In short, this was a true test of "day-zero" protection. This is similar to what Cisco has seen with earlier exploits and worms—the default Cisco Security Agent configuration stopped the exploit, with no binary or policy updates required. The following is a partial list of prior worms and exploits that Cisco Security Agent has stopped via the default security policy settings:

Adobe Flash	Application vulnerability
ANI 0Day	OS vulnerability
Bagle	E-mail worm
BigYellow	Network worm

Blackworm	Network worm
Blaster	Network worm
Bugbear	E-mail worm
Code Red	Network worm
Debploit	Network worm
Fizzer	E-mail worm
Gator/Gain	Spyware
Hotbar	Spyware
HTTP Dir Traversal	Web server vulnerability
IE Text Range	Application vulnerability
IE VML BO	Application vulnerability
SQL Slammer	Network worm
SQL Snake	Network worm
JPEG/GDI+	Malware downloader
MyDoom	E-mail worm
MS06-035	OS vulnerability
MS06-040	OS vulnerability
MS06-070	OS vulnerability
MS07-014	Application vulnerability
Excel hlink dll	Application vulnerability
MS RDS ActiveX	OS vulnerability
MS XML Core Svs	OS vulnerability
Nimda	Network worm
Pentagone/Gonner	E-mail worm
Sasser	Network worm
Sircam	E-mail worm
Sobig	E-mail worm
Storm Trojan	E-mail worm
WMF 0day	OS vulnerability
Word BO	Application vulnerability
W32.Rinbot.H	Network worm
Zotob	Network worm

This exploit is only the latest example of new and mutating attacks that can seriously affect an organization's computing and network environments. The key to stopping these new attacks is two-fold: the ability to stop the attack without requiring any changes to the default configuration, and multiple rules in the default policies that provide defense in depth.

## References

- [1] Microsoft: <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>
- [2] CERT advisory: <http://www.kb.cert.org/vuls/id/827267>



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, COBNT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumina, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn and Cisco Store are service marks, and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDE, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco ICS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, IPPhone, IQStudy, iWeb, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, ProConnect, SmartShore, SlideShow, SMI, SmartNet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (081216)