

Cisco Security Agent and the Microsoft Windows Workstation Service Vulnerability (MS06-070)

PB382503

Summary

A critical vulnerability was announced on November 14, 2006 for Microsoft Windows 2000 and Windows XP operating systems. [1] This vulnerability is actively being exploited. A remote code execution vulnerability exists in the Workstation service that could allow an attacker who successfully exploited this vulnerability to seize control of an affected system. Microsoft has released an update and is recommending customers with affected systems patch immediately. [2]

This vulnerability has already been exploited in several attacks. Cisco® has obtained exploit files, and has confirmed that the Cisco Security Agent is effective in stopping these exploits, using the default security policy configuration. Current supported versions of Cisco Security Agent 4.5.x, 5.0.x, and 5.1.x are all effective in stopping the exploits seen to date.

Details of the Vulnerability

This is a remote code execution vulnerability caused by an unchecked buffer in the Workstation service. Local file system requests and remote file or print network requests are routed through the Workstation service. This service determines where the resource is located and then routes the request to the local file system or to the networking components. When the Workstation service is stopped, all requests are assumed to be local requests.

On Windows 2000, any anonymous user could deliver a specially crafted message to the affected system to exploit this vulnerability. On Windows XP Service Pack 2, the attack could be successfully performed by a user with administrator privileges. [3]

An attacker who successfully exploits this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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.

The following actions have been observed being blocked by Cisco Security Agent running the default security policies:

- Access of registry keys by a suspicious remote application
- Execution of a system function from a buffer, through a buffer overflow

This testing on Windows 2000 Service Pack 4 is shown in Figure 1.

Note that the exploit was tested at Cisco, with the agent in Test 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 Agent 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:

Bagle	E-mail worm	SQL Snake	Network worm
Blaster	Network worm	JPEG/GDI+	Malware downloader
Bugbear	E-mail worm	MyDoom	E-mail worm
Code Red	Network worm	Nimda	Network worm
Debplot	Network worm	Pentagone/Gonner	E-mail worm
Fizzer	E-mail worm	Sasser	Network worm
Gator/Gain	Spyware	Sircam	E-mail worm
Hotbar	Spyware	Sobig	E-mail worm
SQL Slammer	Network worm	Zotob	Network worm

This exploit is only the latest example of new and mutating attacks that can seriously impact 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.

Figure 1. Cisco Security Agent Default Configuration Stops the Microsoft Windows MS06-070 Exploit (Tested on Cisco Security Agent 5.1)

Management Center for Cisco Security Agents V5.1 - Microsoft Internet Explorer

Address: https://localhost/csam51/webadmin

CISCO SYSTEMS Management Center for Cisco Security Agents V5.1

Events Systems Configuration Analysis Maintenance Reports Search Help

Events per page: 50
Sort by: Order received
Filter out similar events: Yes (filtered out ~0% of 2 events)

#	Date	Host	Severity	Event
2	11/19/2006 8:25:33 PM	w2kadvsp4	Notice	TESTMODE: The process 'C:\WINNT\system32\services.exe' (as user NT AUTHORITY\ANONYMOUS LOGON) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINNT\system32\services.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details Rule 182 Wizard Find Similar
1	11/19/2006 8:25:33 PM	w2kadvsp4	Alert	TESTMODE: The process '<remote application>' (as user NT AUTHORITY\ANONYMOUS LOGON) attempted to access the registry key '\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName' and value ''. The attempted access was an open (operation = OPEN/KEY). The operation would have been denied. Details Rule 57 Wizard Find Similar

No rule changes pending [Generate rules](#) Logged in as: admin

References:

- [1] Microsoft Security Advisory: <http://www.microsoft.com/technet/security/bulletin/ms06-070.msp>
- [2] Microsoft Security Advisory: <http://www.microsoft.com/technet/security/bulletin/ms06-070.msp>
- [3] CERT: <http://www.kb.cert.org/vuls/id/778036>



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)