



Product Bulletin No. 3245

Cisco Security Agent and the Microsoft WMF Exploit

SUMMARY

A critical vulnerability was announced on December 27, 2005 for the code used to view picture and fax files in multiple versions of Microsoft Windows operating systems. Microsoft has released a patch for Windows 2000/SP4, Windows XP, and Windows 2003. It is currently unclear whether earlier versions of Windows 2000 or Windows NT are vulnerable. The patch is available from Microsoft [1] at <http://www.microsoft.com/technet/security/Bulletin/MS06-001.msp>.

Many exploits are circulating in the wild and targeting this vulnerability. An exploit creation utility is also circulating, allowing the exploit to mutate rapidly. Cisco Systems® has obtained many 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 are 4.0.3.737, 4.5.1.639, and 5.0.0.176. All are effective in stopping the exploits seen to date.

Cisco has received independent confirmation that Cisco Security Agent is effective in stopping WMF exploits. See Priveon [2], <http://www.priveon.com/rr/whitepapers/CSA%20Protection%20-%20WMF%20Exploit.pdf>.

DETAILS OF THE VULNERABILITY

The vulnerability is in a Windows API most frequently used by a utility shipped with Windows XP SP1 and SP2, and Windows 2003. The utility allows users to view picture and fax files. Malicious files with the extension .wmf that are viewed in Internet Explorer or other applications can execute arbitrary code with SYSTEM privilege. It is possible that malicious files without the .wmf extension could cause a vulnerable application to execute and be exploited due to the header information in the file. Many Trojan horse programs are using this to download and compromise systems. Applications known to be vulnerable include Internet Explorer, Windows Explorer, Outlook, Lotus Notes, and the Google Desktop Search (GDS) (if it indexes a file containing exploit code).

The CERT advisory [3] states that most e-mail clients are likely able to be exploitable in this way.

Once an exploit begins to execute code, it typically performs many malicious actions, including (but not limited to):

- Downloading malware files
- Installing software that automatically starts at boot time (RUN or RUNONCE Registry keys)
- Executing command shells such as CMD.EXE
- Capture keystrokes typed by the user

The specific types and sequences of malicious activity used will vary from exploit to exploit.

HOW CISCO SECURITY AGENT STOPS THE WORM

The Cisco Security Agent default policies contain at least five rules that stop the exploit and variants. The exact number of malicious activities that is stopped varies depending on the variant tested, but up to 60 behaviors were identified during testing at Cisco (using the XLP1.WMF variant). 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:

- Execution of a system function from a buffer, via a buffer overflow
- Execution of a downloaded executable
- The attacked service attempted to execute a command shell (CMD.EXE)
- An executable file (or files) was written to the %SYSTEM directory
- One of the downloaded executables attempted to capture keystrokes
- The application executed from the file tried to create RUN registry entries

This testing 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. Cisco tested with agents in Test mode to determine how deep the Cisco Security Agent defense in depth is for the exploits and variants. For the XLP1.WMF variant, this defense in depth is over 60 (Figure 1 contains only a partial screen capture due to the volume of data).

Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for CSA agents to be effective. In short, this was a true test of “Day Zero” protection. This is similar to what we have 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 the Cisco Security Agent has stopped via the default security policy settings:

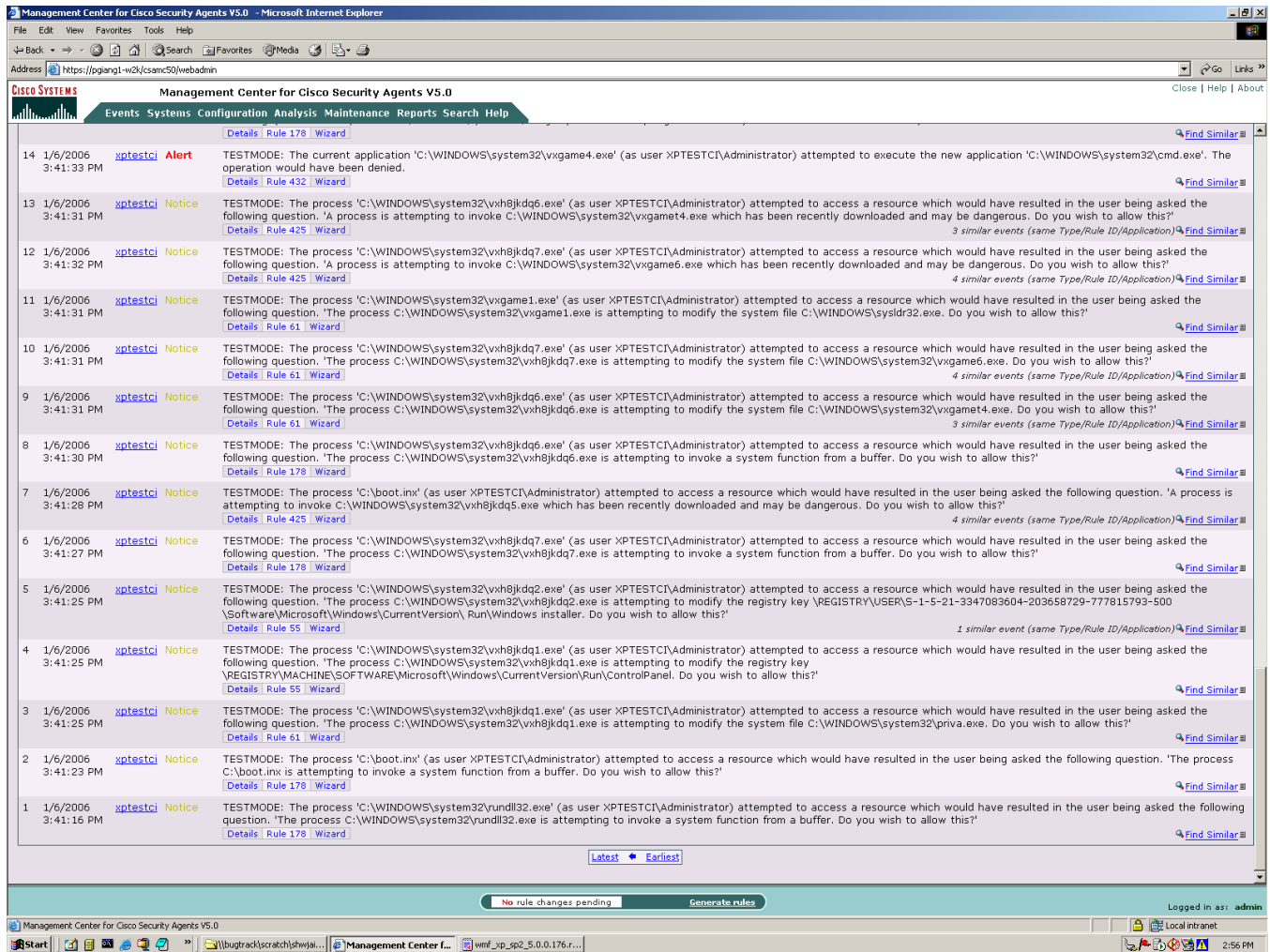
Bagle: Email worm	SQL Snake: Network worm
Blaster: Network worm	JPEG/GDI+: Malware downloader
Bugbear: Email worm	MyDoom: Email worm
Code Red: Network worm	Nimda: Network worm
Debploit: Network worm	Pentagone/Gonner: Email worm
Fizzer: Email worm	Sasser: Network worm
Gator/Gain: Spyware	Sircam: Email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

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

OBSERVED ANOMALIES

Cisco observed two anomalous situations during testing. One was during testing on benign (non-malicious) proof-of-concept code. Since this limited itself to executing the calculator application (CALC.EXE), it did not trigger protective rules. This is by intent—the security policies are designed to block malicious activity, as opposed to interesting but harmless activity. The second situation occurred while testing a malicious exploit, where a three-minute delay was observed between execution of the exploit and generation of events by Cisco Security Agent. Cisco believes that the exploit was searching memory addresses during this interval, and had not yet executed malicious behavior. Once the exploit performed malicious activities, Cisco Security Agent blocked the activities as expected.

Figure 1. Cisco Security Agent Default Configuration Stops the WMF Exploit (XPL1.WMF variant). First 14 event captures (of 61 total). Tested on Cisco Security Agent 5.0.0.176



REFERENCES:

- [1] Microsoft: <http://www.microsoft.com/technet/security/Bulletin/MS06-001.msp>
- [2] Priveon: <http://www.priveon.com/tr/whitepapers/CSA%20Protection%20-%20WMF%20Exploit.pdf>
- [3] CERT: <http://www.kb.cert.org/vuls/id/181038>

The Register: http://www.theregister.co.uk/2005/12/29/wmf_trojan_alert/

Gibson Research: <http://www.grc.com/sn/notes-020.htm>



Corporate 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: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

C25-336465-00 02/06