

Cisco Security Agent and the Microsoft Win32/Nuwar.N (Storm Trojan) Exploit

PB398745

Summary

Win32/Nuwar.N@MM!CME-711 is a mass-mailing email worm that sends a Trojan via email. This exploit affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, and Windows XP operating systems. This worm was first discovered on January 19, 2007. Different antivirus vendors have been using different names to refer to this exploit: CME-711, W32/Downloader.AYDY (F-Secure), Troj/DwnLdr-FYD (Sophos), Trojan.Peacomm (Symantec), Win32/Pecoan, Win32/Pecoan.B, Win32/Pecoan.E, Win32/Pecoan.F, Win32/Pecoan.G, and Downloader-BAI.sys!M711 (McAfee).

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

When the Trojan attachment is opened, it downloads a copy of the email worm component. The email component is encrypted. It drops and installs wincom32.sys, which loads and infects a dll into the memory process of services.exe. The dll contains the capability to scan various UDP ports to create a peer-to-peer (P2P) network with other infected computers for the purpose of downloading and updating. The P2P network can then be used by a malicious user to retrieve information on what files to download and execute. It also retrieves information of additional peers and updates its own peer list file with the gathered information. Known other components downloaded are other Win32/Nuwar variants.¹

¹ References:

Microsoft: <http://www.microsoft.com/security/encyclopedia/details.aspx?Name=Win32/Nuwar.N@mm>

The email composed by Win32/Nuwar.N@MM!CME-711 has the following characteristics:

- **Subject (may be one of the following):**
 - 230 dead as storm batters Europe.
 - A killer at 11, he's free at 21 and kills again!
 - British Muslims Genocide
 - Naked teens attack home director.
 - Re: Your text
 - Russian missile shot down USA satellite
 - U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel.
- **Message body:**
 - blank
- **Attachment name:**
 - FullClip.exe
 - Full Story.exe
 - FullVideo.exe
 - Read More.exe
 - Video.exe

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 a system file by a recently downloaded application
- Modification of system files by a suspicious remote application
- Execution of a system function from a buffer, through a buffer overflow
- Modification of kernel functionality
- Initiating a client connection across various UDP ports (UDP Ports 137, 53, 6121, 18559, 2581, 3620)

This testing is shown in Figure 1 and 2.

Note: 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 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 table 1 is a partial list of prior worms and exploits that Cisco Security Agent has stopped through the default security policy settings.

Table 1.

Security Agent	Worm	Security Agent	Worm
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
Debploit	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 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.

Figure 1. Figure 1. Cisco Security Agent Default Configuration Stops the Storm Trojan Exploit (Tested on Cisco Security Agent 5.1)



