

Cisco Security Agent and Win32.Rinbot.H exploit

PB402473

Summary

W32.Rinbot.H is a worm that spreads through network shares and by exploiting certain vulnerabilities. It also opens a back door on the compromised computer. This exploit affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP operating systems. This worm was first discovered on February 26, 2007.

This vulnerability has already been exploited in several attacks. Cisco® has obtained exploit files, and has confirmed that 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

W32.Rinbot.H is a worm affecting Windows platforms. This worm also contains back-door functionality, allowing a malicious user remote access to the infected computer through IRC channels while running in the background.

When the worm executes, it copies itself to the following location:

```
%System%\mstsc.exe
```

Next, the worm creates the following registry entry so that it executes whenever Windows starts:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"Terminal Services" = %System%\mstsc.exe"
```

The worm may spread through network shares protected by weak passwords and by exploiting the following vulnerabilities:

- Symantec Client Security and Symantec Antivirus Elevation of Privilege (BID 18107)
- Microsoft Windows Server Service Remote Buffer Overflow Vulnerability (BID 19409)
- Microsoft SQL Server User Authentication Remote Buffer Overflow Vulnerability (BID 5411) using UDP port 1434¹

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.

¹ Symantec: http://www.symantec.com/en/ca/smb/security_response/writeup.jsp?docid=2007-022615-1754-99&tabid=1

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, through a buffer overflow
- Modification of system files by a recently downloaded application
- Modification of registry keys
- Modification of system memory

This testing is shown in Figures 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 following is a partial list of prior worms and exploits that Cisco Security Agent has stopped via the default security policy settings:

Table 1.

Exploit	Worm	Exploit	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. Cisco Security Agent Default Configuration Stops the Win32.Rinbot.H Exploit (Tested on Cisco Security Agent 5.1)

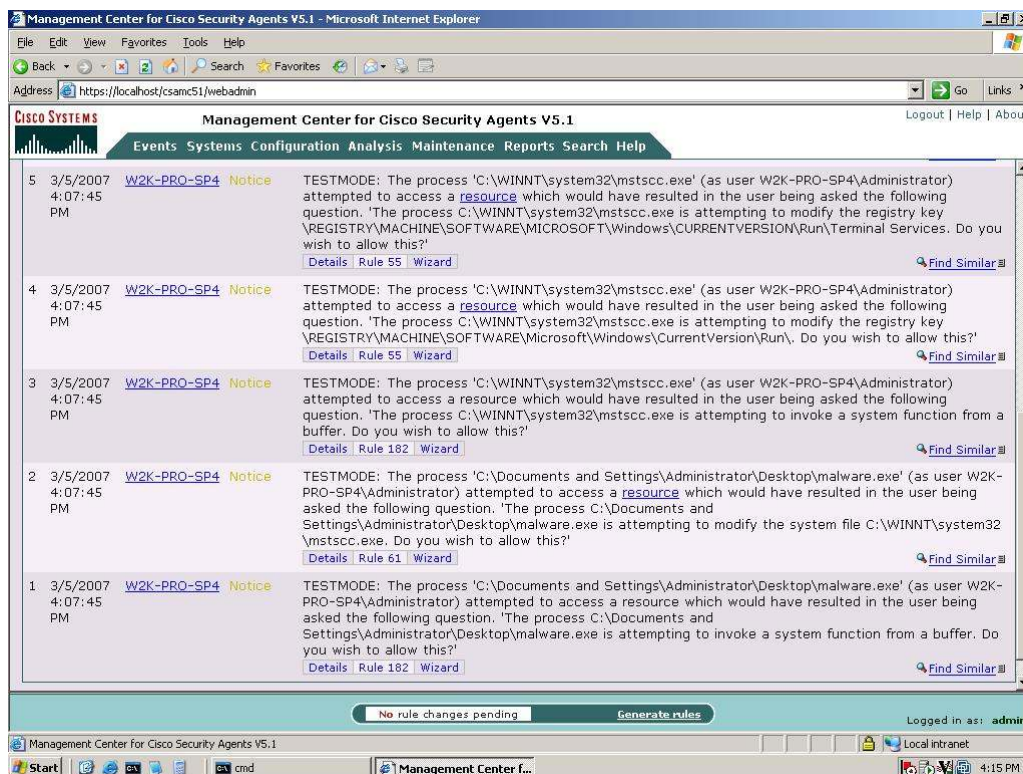
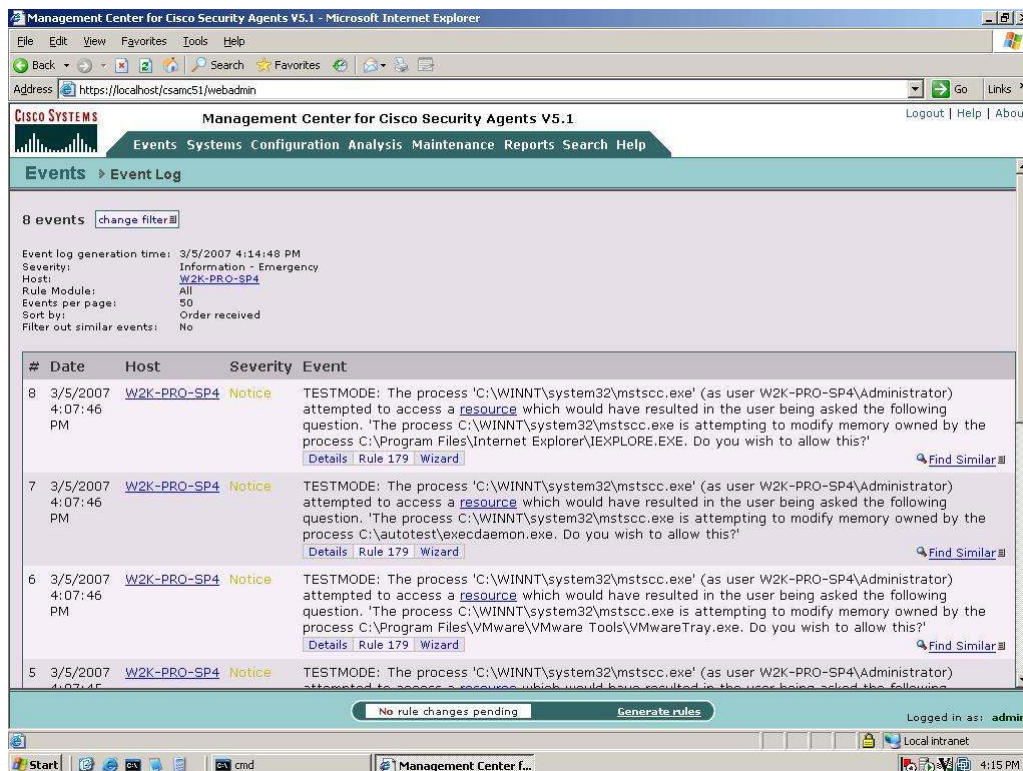


Figure 2. Cisco Security Agent Default Configuration Stops the Win32.Rinbot.H Exploit (Tested on Cisco Security Agent 5.1)





Americas Headquarters
 Cisco Systems, Inc.
 170 West Taftman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 520-4000
 800 653-1715 (toll-free)
 Fax: 408 527-0689

Asia Pacific Headquarters
 Cisco Systems, Inc.
 155 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
 Heerlenbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www.europe.cisco.com
 Tel: +31 20 620 0791
 Fax: +31 20 657 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.

©2007 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, Register, Abroad, EPC, Catalyst, CSDA, CCIP, 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, Diagnose/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, Gigamon, GigaStack, HomeLink, Internet Quotient, IQS, iPhone, iRTV, IQ Director, the IQ logo, IQ Net, Roadshow, Scorecard, Quick Study, iQoS, iStream, iLinksys, iMeetingPlace, iMGX, iNetworking Academy, iNetwork Register, iPacket, iPK, iProConnect, iRabbit, iUX, iScriptShare, iVoiceCast, iVARTNet, iBackWire, iThe Router, iWay to Increase Your Internet Quotient, and iThreatPath 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. (07012)