

Cisco Security Agent and the Symantec Big Yellow Botworm

PB389319

Summary

A new worm, code-named "Big Yellow", was discovered on December 15, 2006. Big Yellow is actively exploiting a remote Symantec buffer overflow vulnerability originally discovered on May 24, 2006. [1] This vulnerability was first publicly exploited by another similar worm on November 30, 2006.

This vulnerability can be found in the Microsoft Windows versions of Symantec Client Security versions 3.0 and 3.1 and Symantec AntiVirus Corporate Edition versions 10.0 to 10.1 products. In a May 2006 advisory, Symantec confirmed that Symantec Client Security and Symantec AntiVirus Corporate Edition are susceptible to a buffer overflow and issued a patch for vulnerable versions.

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

The Big Yellow worm exploits the Symantec buffer overflow vulnerability and turns vulnerable computers into remote-controlled zombies. The new "botworm" scans for computers running the vulnerable Symantec software and then attempts to break in. [2] An attacker who successfully exploits this vulnerability could remotely take complete control of an affected system. The attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

A similar worm, a variant of Spybot, spread in November 2006. When installed on a PC, both Spybot and Big Yellow were observed to open a back door in the system and connect to an Internet Relay Chat server to let the remote attacker control the compromised computer. Such remote control software is the most prevalent threat to Windows PCs, according to Microsoft. [2]

The Symantec buffer overflow vulnerability being exploited by the Big Yellow "botworm" is due to a boundary error in the remote management interface when processing "COM_FORWARD_LOG" commands. This can be exploited to cause a stack-based buffer overflow via a specially crafted "COM_FORWARD_LOG" command sent to port 2967/tcp. [3]

How Cisco Security Agent Stops the Exploit

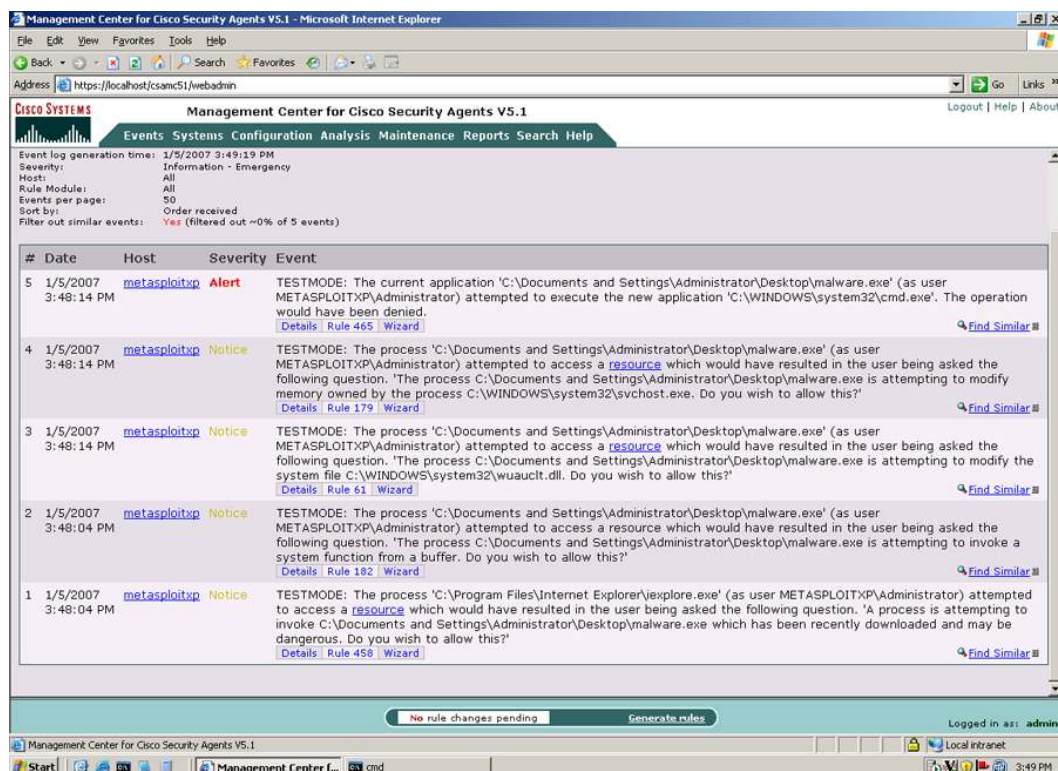
Cisco Security Agent default policies contain multiple rules that stop the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection.

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

- Modification of system files by a suspicious remote application
- Execution of a system function from a buffer, through a buffer overflow
- Execution of a suspicious application

This testing is shown in Figure 1.

Figure 1. Cisco Security Agent Default Configuration Stops the Symantec Big Yellow Botworm Exploit (Tested on Cisco Security Agent 5.1)



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:

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.

References:

- [1] eEYE Digital Security: <http://research.eeye.com/html/alerts/AL20061215.html>
- [2] CNET News: http://news.com.com/New+botworm+exploits+Symantec+flaw/2100-1002_3-6144282.html
- [3] Secunia Advisory: <http://secunia.com/advisories/20318>



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.

©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 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, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuickStudy, 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. (0701R)