



Product Bulletin No. 367645

## Cisco Security Agent and the Microsoft Internet Explorer VML Buffer Overflow (MS06-55)

### SUMMARY

A critical “day-zero” vulnerability was announced on September 26, 2006 for Microsoft Windows XP and XP Professional, Windows Server 2003, and Windows Server 2003 x64. The vulnerability is found in the Internet Explorer code base on these platforms and follows Internet Explorer standards for packaging, detection, and deployment [1]. This vulnerability is actively being exploited. Microsoft has released patches for this vulnerability and is recommending that customers patch their affected systems immediately.

This vulnerability has already been exploited in several attacks. Cisco Systems® has obtained exploit files, and has confirmed that Cisco® Security Agent is effective in stopping these exploits, using the default security policy configuration. No changes to the default configuration or policy updates were required to receive this protection. Current supported Cisco Security Agent versions 4.0.3.x, 4.5.1.x, 5.0.0.x, and 5.1.0.x are effective in stopping the exploits seen to date.

### DETAILS OF THE VULNERABILITY

Microsoft Internet Explorer 5.0 and higher supports Vector Markup Language (VML), which is a set of Extensible Markup Language (XML), tags for drawing vector graphics. Internet Explorer fails to properly handle malformed VML tags, which allows a stack buffer overflow to occur. The CERT advisory [2] states that if a remote attacker can persuade a user to access a specially crafted Webpage with Internet Explorer, that attacker may be able to trigger the buffer overflow. In addition, an attacker could deliver an HTML email message or entice a user to select an HTML document in Windows Explorer.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

### HOW CISCO SECURITY AGENT STOPS THE EXPLOIT

Cisco Security Agent default policies contain three different rules that stopped 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 (downloaded) application
- Execution of a system function from a buffer, through a buffer overflow

This testing is shown in Figure 1.

The exploit was tested at Cisco with Cisco Security Agent in Test mode, which does not block malicious behavior. This allows the agent to report all rules that would be applied if the agent was in protect mode, 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.

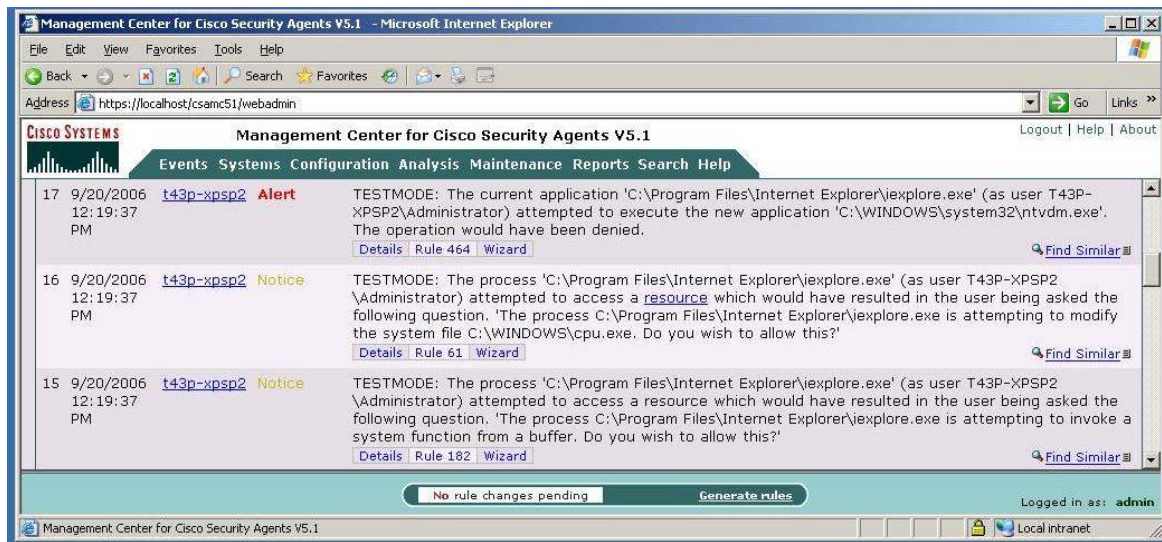
Testing was performed against the Cisco Security Agent default policies. No binary or policy update was needed for Cisco Security Agents to be effective. In short, this was a true test of “day-zero” protection. This is similar to what we have seen with earlier exploits and

worms—the default Cisco Security Agent configuration stopped the exploit, with no binary or policy updates required. Following is a partial list of prior worms and exploits that Cisco Security Agent has stopped using 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 the ability to stop the attack without requiring any changes to the default configuration, and to have multiple rules in the default policies that provide defense in depth.

**Figure 1.** Cisco Security Agent 5.1 Default Configuration Stops the Microsoft Internet Explorer VML Buffer Overflow Exploit



## REFERENCES

1. Microsoft Security Advisory 925568: <http://www.microsoft.com/technet/security/advisory/925568.mspx>.
2. CERT Vulnerability Note VU# 416092: <http://www.kb.cert.org/vuls/id/416092>.



**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](http://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, 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, 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)