

Cisco Security Agent and the Adobe Flash Player Vulnerability (CVE-2007-0071)

Summary

The Adobe Flash Player is a player for the Flash media format and enables frame-based animations and multimedia to be viewed within a web browser. There are reports of a critical vulnerability affecting current versions of Adobe Flash and evidence of it being exploited in the wild. Versions prior to 9.0.124.0 are reported to be at risk.

Cisco has obtained exploit files and has confirmed that Cisco[®] Security Agent is effective in stopping this exploit using the default security policy configuration.

Details of the Adobe Flash Player Vulnerability

Adobe Flash Player is vulnerable to a buffer overflow, caused by an integer overflow vulnerability in the processing of multimedia files. By creating a specially crafted multimedia file and persuading the victim to open the file, a remote attacker could overflow a buffer and execute arbitrary code on the system.

The integer overflow vulnerability is detailed in CVE-2007-0071¹. An attacker may be able to trigger this overflow by convincing a user to open a specially crafted SWF file. The SWF file could be hosted or imbedded in a webpage.

How Cisco Security Agent Stops the Exploit

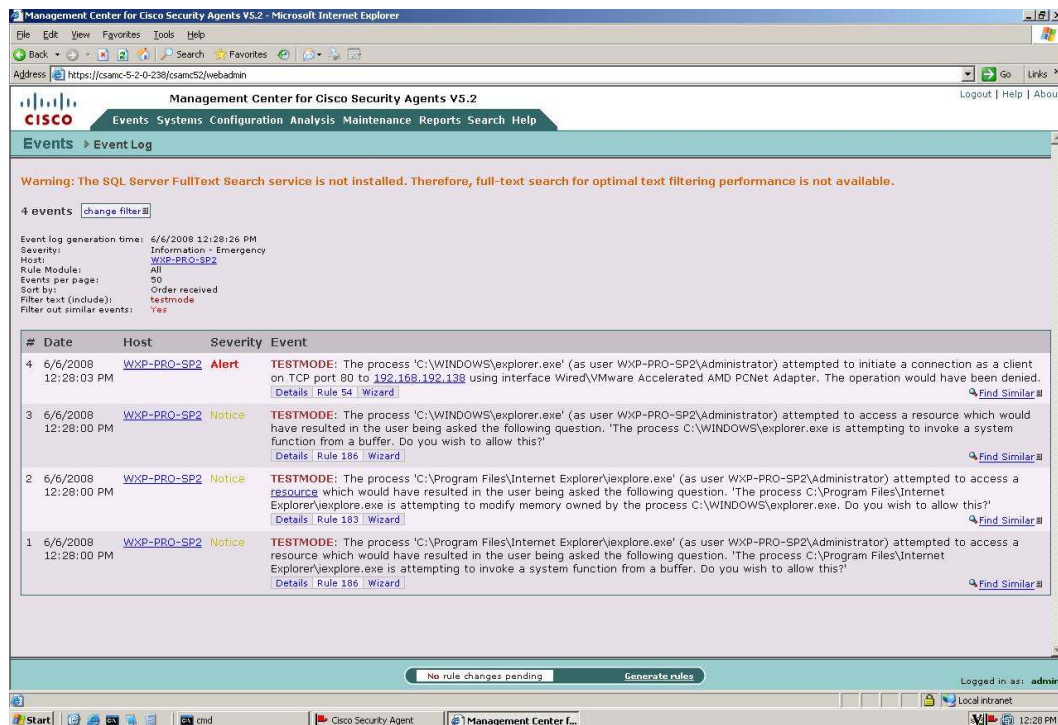
Cisco Security Agent default policies contain multiple rules that stop the exploit from doing any damage. No changes to the Cisco Security Agent binaries or default configuration are required to get this protection. The following actions have been observed being blocked by Cisco Security Agent running the default security policies:

- An attempt to invoke a system function from a buffer
- An attempt to modify memory owned by the process C:\WINDOWS\explorer.exe
- An attempt to establish a client connection over the network on TCP Port 80

The testing is shown in Figure 1.

¹ National Vulnerability Database—NIST: <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-0071>

Figure 1. Cisco Security Agent Default Configuration Stops the Adobe Flash Vulnerability Exploit (Tested on Cisco Security Agent 5.2.0.238 with the Default Desktop Group)



Note: The exploit was tested at Cisco by the Security Intelligence Engineering and Cisco Security Agent teams 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 "zero-day" 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 using the default security policy settings:

Table 1.

Exploits	Worms	Exploits	Worms
ANI 0Day	OS vulnerability	MyDoom	Email worm
Bagle	Email worm	MS06-035	OS vulnerability
BigYellow	Network worm	MS06-040	OS vulnerability
Blackworm	Network worm	MS06-070	OS vulnerability
Blaster	Network worm	MS07-014	Application vulnerabilities
Bugbear	Email worm	Excel hlink dll	Application vulnerability
Code Red	Network worm	MS RDS ActiveX	OS vulnerability
Debplot	Network worm	MS XML Core Svs	OS vulnerability
DNS 0Day	OS vulnerability	Nimda	Network worm
Fizzer	Email worm	Pentagone/Gonner	Email worm

Exploits	Worms	Exploits	Worms
Gator/Gain	Spyware	Sasser	Network worm
Hotbar	Spyware	Sircam	Email worm
HTTP Dir Traversal	Web server vulnerability	Sobig	Email worm
IE Text Range	Application vulnerability	Storm Trojan	Email worm
IE VML BO	Application vulnerability	WMF 0day	OS vulnerability
SQL Slammer	Network worm	Word BO	Application vulnerability
SQL Snake	Network worm	W32.Rinbot.H	Network worm
JPEG/GDI+	Malware downloader	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.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0805R)