



Product Bulletin No. 3275

Cisco Security Agent and the Microsoft Internet Explorer createTextRange() Exploit

SUMMARY

A critical vulnerability was announced on March 23, 2006 for Microsoft Internet Explorer versions 5.01, 5.5, and 6.0. [1] This vulnerability is actively being exploited. An unpatched vulnerability in the way that Internet Explorer renders HTML could allow attackers to seize control of the system. This vulnerability affects systems running Windows 2000, Windows XP, Windows 98, and Windows Server 2003. Microsoft has announced it will release a fix for this in its already scheduled April 11, 2006 security update.

This vulnerability has already been exploited in several attacks. Cisco Systems® 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 are 4.0.3.737, 4.5.1.639, and 5.0.0.176. All are effective in stopping the exploits seen to date.

DETAILS OF THE VULNERABILITY

The vulnerability relates to the way that Internet Explorer processes information using the createTextRange() method. The createTextRange() method is a dynamic HTML (DHTML) method that is exposed by the DHTML Object Model [2]. By presenting the browser with specially crafted code, attackers could corrupt the system memory and trick it into running unauthorized software.

The CERT advisory [3] states that by convincing a user to open a specially crafted Webpage, a remote unauthenticated attacker can execute arbitrary code on a vulnerable system. Known attack vectors for this vulnerability require Active Scripting to be enabled. By disabling Active Scripting, the chances of exploitation are reduced.

HOW CISCO SECURITY AGENT STOPS THE EXPLOIT

The Cisco Security Agent default policies contain a buffer overflow prevention rule that stops 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:

- Execution of a system function from a buffer, via a buffer overflow

This testing is shown in Figure 1.

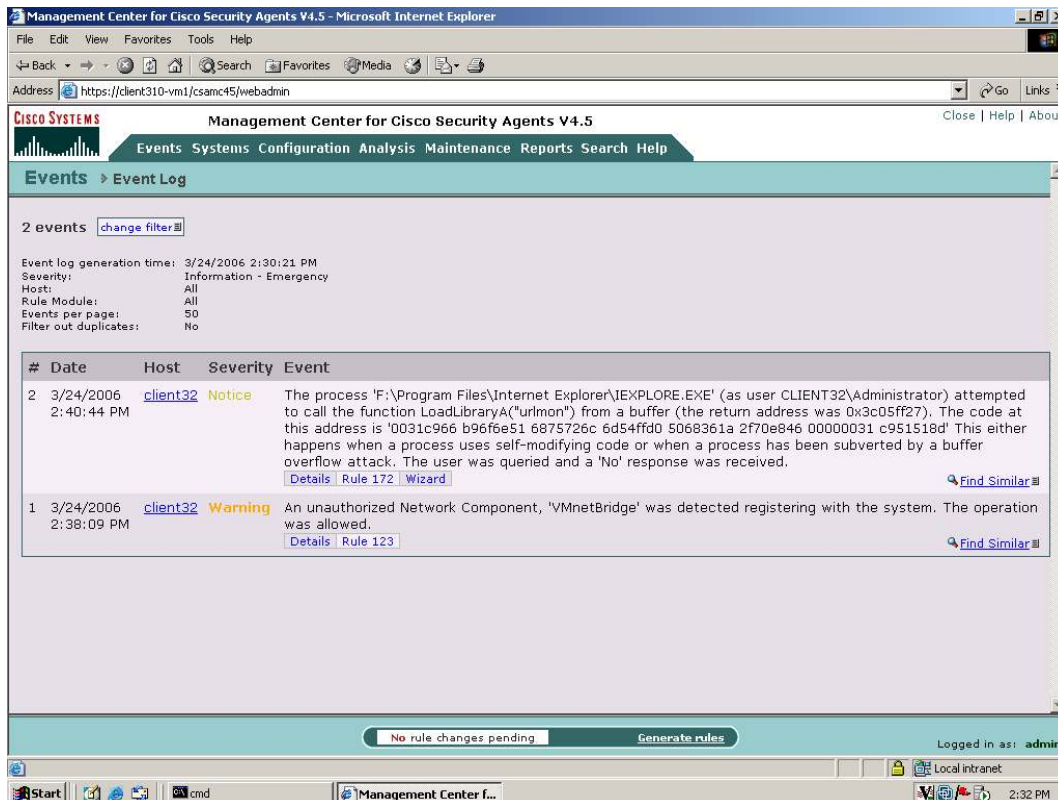
Note that the exploit was tested at Cisco, with the agent in Test mode, which will cause the agent to alert (but not block) malicious behavior. This was done to observe all possible ways that the Cisco Security Agent default policies would stop the exploit. When the agent is in protect mode (the typical 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 Agent 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 impact organization's computing and network environments. The key to stopping these new attacks is twofold: the ability to stop the attack without requiring any changes to the default configuration, and multiple rules in the default policies that provide a defense in depth.

Figure 1. Cisco Security Agent Default Configuration Stops the Microsoft Internet Explorer createTextRange() Exploit (Tested on Cisco Security Agent 4.5)




REFERENCES:

- [1] Microsoft Security Advisory: <http://www.microsoft.com/technet/security/advisory/917077.msp>.
- [2] Microsoft DHTML: http://msdn.microsoft.com/library/default.asp?url=/workshop/author/dhtml/dhtml_node_entry.asp.
- [3] CERT: <http://www.kb.cert.org/vuls/id/876678>.
Securing Your Web Browser: http://www.us-cert.gov/reading_room/securing_browser/.
Secunia Advisory: <http://secunia.com/advisories/18680/>.



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.**

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)

Printed in USA

C25-347327-00 05/06