

Cisco Security Agent and Microsoft September 2007 Security Bulletin Release

PB430478

Summary

Microsoft released the September 2007 Security Advisory Bulletin on August 14, 2007. Four bulletins were released that address four individual vulnerabilities.

Details of the August Bulletin

Details of the vulnerabilities are documented by Microsoft¹. The one bulletin rated as Critical addresses remote code execution vulnerabilities in Microsoft Agent affecting the Windows 2000 operating system. Microsoft also released three bulletins rated as Important to correct vulnerabilities in remote code execution for Microsoft Visual Studio and MSN Messenger and Windows Live Messenger, and an escalation of privilege vulnerability in Windows Services for UNIX and Subsystem for UNIX-based Applications. Attackers must rely on user interaction to exploit the two arbitrary code execution vulnerabilities. This factor reduces the potential for exploitation.

Cisco Security Agent Response

Cisco Security Agent offers proactive protection against exploits and variants that are trying to take advantage of published and unpublished vulnerabilities. Cisco Security Agent is designed to protect servers, desktops, and POS devices from these threats by using rules-based policies. This allows customers to have protection against new and unknown threats without having to update the product with attack-based "signatures."

The following is an estimation of how endpoints protected by Cisco Security Agent will perform when faced with attacks based on these newly disclosed vulnerabilities using the Cisco provided default policies. No actual exploit testing using these vulnerabilities has been performed to date so there may be a difference in the real-world Cisco Security Agent test results against actual exploits.

Critical

MS07-051: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)

Based on the information provided in the Microsoft advisory, this vulnerability is similar to a prior Microsoft XML Core Services ActiveX vulnerability (CVE-2006-5745). It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against CVE-2006-5745 by an independent third party

<http://www.priveon.com/dmdocuments/PV-A-060005A.pdf>.

¹ Microsoft: <http://www.microsoft.com/technet/security/bulletin/ms07-sep.msp>

Important**MS07-052: Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution (941522)**

Based on the information provided in the Microsoft advisory, this vulnerability is similar to prior Microsoft Word vulnerabilities (CVE-2006-5994). It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against MS07-014

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8060b074.html.

MS07-053: Vulnerability in Windows Services for UNIX Could Allow Elevation of Privilege (939778)

Since currently shipping versions of Cisco Security Agent do not run on Windows Services for UNIX, Cisco Security Agent would not provide protection against this vulnerability.

MS07-054: Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution (942099)

Based on the information provided in the Microsoft advisory, the MSN Messenger and Windows Live Messenger vulnerabilities are similar to a prior Microsoft Win32/Nuwar.N e-mail worm (Storm Trojan). It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against the Storm Trojan exploit

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8060adea.html.



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, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, 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. (0708R)