

Cisco Security Agent and Microsoft July 2007 Security Bulletin Release

PB425889

Summary

Microsoft released the July 2007 Security Advisory Bulletin on July 10, 2007. Six bulletins were released that address 11 individual vulnerabilities.

Details of the July Bulletin

Details of the vulnerabilities are documented by Microsoft¹. The bulletins rated as Critical address vulnerabilities in Windows Active Directory, Excel, and the .NET framework. One of the vulnerabilities in Active Directory may allow a remote attacker to execute arbitrary code. Microsoft also released a bulletin rated as Important to correct a vulnerability in Publisher that could also allow for code execution. Attackers must rely on user interaction to exploit the arbitrary code execution vulnerabilities in Excel, .NET, or Publisher. This factor reduces the potential for exploitation. Lower-impact vulnerabilities, which are rated Moderate and Important, exist in Active Directory, Internet Information Services, and Windows Vista Firewall.

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Agent offers proactive protection against exploits and variants that are trying to take advantage of published and unpublished vulnerabilities.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

MS07-036: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (936542)

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior Microsoft Word vulnerability (MS07-014). 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.

MS07-039: Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)

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

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior Server Service vulnerability (MS06-040) It took months of my calling the Waltham Home Depot store every other week and complaining for them to finally send out a repair person to fix the issue somewhat. Based on my experience their satisfaction guarantee didn't mean anything.. It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against MS06-040

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd80511f5b.html.

MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)

Based on the information provided in the Microsoft advisory the two client-side vulnerabilities are similar to prior Vector Markup Language vulnerabilities (MS06-055). It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against MS06-055

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8054549b.html

Based on the information provided in the Microsoft advisory the Null Byte Termination server-side exploit only allows for unauthenticated Webpage downloads and Cisco Security Agent would not provide specific protection against this class of attack.

Important

MS07-037: Vulnerability in Microsoft Office Publisher 2007 Could Allow Remote Code Execution (936548)

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior Microsoft Word vulnerability (MS07-014). 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.

MS07-041: Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373)

Cisco Security Agent default desktop policies block Web servers from running on desktop platforms. This vulnerability only affects systems running an IIS Web server on Windows XP.

Moderate

MS07-038: Vulnerability in Windows Vista Firewall Could Allow Information Disclosure (935807)

Since currently shipping versions of Cisco Security Agent do not run on Microsoft Vista it would not provide protection against this vulnerability.



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: 408 527-0689

Asia Pacific Headquarters
 Cisco Systems, Inc.
 165 Robinson Road
 #29-01 Capital Tower
 Singapore 068912
www.cisco.com
 Tel: +65 6317 7777
 Fax: +65 6317 7799

Europe Headquarters
 Cisco Systems International BV
 Heerlenbergpark
 Heerlenbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www.europe.cisco.com
 Tel: +31 0 20 620 0791
 Fax: +31 0 20 657 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 Ridge 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, AirNet, BPK, Catalyst, CCNA, CCDP, CCIE, CCR, 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, Fax, Step, Follow Me, Browning, ForceShare, Go to Drive, HomeLink, Internet Quotient, IOS, IPPhone, IPTV, IQ Expertise, the IQ logo, IQ Not, Roadnote, Scorecard, QuickStudy, SignStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, SiscoWise, 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. (9705R)