

## Cisco Security Agent and Microsoft August 2007 Security Bulletin Release

PB425877

### Summary

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

### Details of the August Bulletin

Details of the vulnerabilities are documented by Microsoft<sup>1</sup>. The six bulletins rated as Critical address remote code execution vulnerabilities in OLE Automation, XML Core Services, Excel, Internet Explorer, Graphics Rendering Engine, and the Vector Markup Language. Microsoft also released three bulletins rated as Important to correct vulnerabilities in remote code execution for Windows Media Player and Windows Gadgets, and an escalation of privilege vulnerability in Virtual PC and Server. Attackers must rely on user interaction to exploit the eight 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Agent offers proactive protection against exploits and variants that are trying to take advantage of published and unpublished vulnerabilities.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

MS07-042: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (936227)

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior Microsoft XML Core Services 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>.

MS07-043: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)

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

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior Vector Markup Language vulnerability (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](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8054549b.html).

MS07-044: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (940965)

Based on the information provided in the Microsoft advisory this Excel 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](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8060b074.html).

MS07-045: Cumulative Security Update for Internet Explorer (937143)

Based on the information provided in the Microsoft advisory the three Internet Explorer vulnerabilities are similar to a prior Vector Markup Language vulnerability (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](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8054549b.html).

MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior GDI vulnerability (MS06-001). It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against MS06-001

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod\\_bulletin0900aecd80420fde.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd80420fde.html)

MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)

Based on the information provided in the Microsoft advisory the three Internet Explorer vulnerabilities are similar to a prior Vector Markup Language vulnerability (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](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd8054549b.html)

### **Important**

MS07-047: Vulnerability in Windows Media Player Could Allow Remote Code Execution (936782)

Based on the information provided in the Microsoft advisory this vulnerability is similar to a prior GDI vulnerability (MS06-001). It is expected that Cisco Security Agent would have similar effectiveness to Remote Code Execution attacks as tested against MS06-001

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod\\_bulletin0900aecd80420fde.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps5057/prod_bulletin0900aecd80420fde.html)

MS07-048: Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution (938123)

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

#### MS07-049: Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (937986)

Since currently shipping versions of Cisco Security Agent do not run on Microsoft Virtual PC and Virtual Server it would not provide protection against these vulnerabilities.



**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.  
155 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 6191  
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](http://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, Airnet, BPK, Catalyst, CCD, CCDA, 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, Fast, Step, Follow Me Browsing, FormShare, Go to Drive, HomeLink, Internet Quotient, IOS, IPPhone, IPTV, IQ Expertise, the IQ logo, IQ Notepad, Scorecard, QuickStudy, SignStream, iInlays, Modeling Place, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, SecureWise, 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)