

Cisco Security Agent and MS07-014— Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (929434)

PB400600

Summary

Critical vulnerabilities in the Microsoft Word application were announced on February 13, 2007 for Microsoft Office 2000, Office XP, Office 2003, and Microsoft Works Suite.¹ These vulnerabilities are actively being exploited. A remote code execution vulnerability could allow an attacker who successfully exploited this vulnerability to seize control of an affected system. Microsoft has released update files and is recommending customers with affected systems patch immediately.

This vulnerability has already been exploited in several attacks. Cisco[®] 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 4.5.x, 5.0.x, and 5.1.x are all effective in stopping the exploits seen to date.

Details of the Vulnerability

If a user is logged on with administrative user rights, an attacker who successfully exploited these vulnerabilities below could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Word Malformed String Vulnerability—CVE-2006-5994:

A remote code execution vulnerability exists in the way Microsoft Word handles Word files with a specially crafted string. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Website. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

Word Malformed Data Structures Vulnerability—CVE-2006-6456:

A remote code execution vulnerability exists in the way Microsoft Word handles Word files with a specially crafted data structure. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Website. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability.

Word Count Vulnerability—CVE-2006-6561:

A remote code execution vulnerability exists in Microsoft Word. An attacker could exploit this vulnerability when Word parses a file and processes an unchecked count. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Website. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote

¹ Microsoft: <http://www.microsoft.com/technet/security/Bulletin/MS07-014.mspx>

code execution. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability.

Word Macro Vulnerability—CVE-2007-0208:

A remote code execution vulnerability exists in Microsoft Word. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Word Malformed Drawing Object Vulnerability—CVE-2007-0209:

A remote code execution vulnerability exists in Microsoft Word. An attacker could exploit this vulnerability when Word parses a file and processes a malformed drawing object. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Website. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

Word Malformed Function Vulnerability—CVE-2007-0515:

A remote code execution vulnerability exists in Microsoft Word. An attacker could exploit this vulnerability when Word parses a file and processes a malformed function. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Website. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

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:

- Modification of system files by a suspicious remote application
- Execution of a system function from a buffer, through a buffer overflow

This testing is shown in Figure 1.

Note: 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 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:

Exploits	Worms	Exploits	Worms
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
Debplot	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 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.

Figure 1. Cisco Security Agent Default Configuration Stops the MS-07-014 Exploit (Tested on Cisco Security Agent 5.1)

The screenshot displays the Management Center for Cisco Security Agents V5.1 web interface. The main content area shows the 'Event Log' with two events. The most recent event (ID 2) is a 'Notice' severity event from host 'WXPPROSP2' on 2/27/2007 at 11:22:46 AM. The event description states: 'TESTMODE: The process 'C:\Program Files\Microsoft Office\Office\WINWORD.EXE' (as user WXPPROSP2\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Program Files\Microsoft Office\Office\WINWORD.EXE is attempting to modify memory owned by the process C:\WINDOWS\explorer.exe. Do you wish to allow this?''. The event is linked to 'Rule 179'.

#	Date	Host	Severity	Event
2	2/27/2007 11:22:46 AM	WXPPROSP2	Notice	TESTMODE: The process 'C:\Program Files\Microsoft Office\Office\WINWORD.EXE' (as user WXPPROSP2\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Program Files\Microsoft Office\Office\WINWORD.EXE is attempting to modify memory owned by the process C:\WINDOWS\explorer.exe. Do you wish to allow this?' Details Rule 179 Wizard Find Similar
1	2/27/2007 11:22:46 AM	WXPPROSP2	Notice	TESTMODE: The process 'C:\WINDOWS\explorer.exe' (as user WXPPROSP2\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\explorer.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details Rule 182 Wizard Find Similar

