Security
April 14, 2009 11:09 AM PDT

Microsoft fills Excel, Windows, Word holes

by Elinor Mills

Updated 12:30 p.m. PDT *with ZoneAlarm discount offer and* ***11:50 a.m. PDT*** *with comment from security vendors.*

Microsoft on Tuesday closed security holes in Excel, Windows, and Word that had been exploited in the wild as well as other holes for which exploit code or details exist, all as part of its monthly patch update cycle.

The critical Excel hole could allow an attacker to take complete control of an unpatched system if a user opens a specially crafted Excel file. Security firm Symantec **said in February** that it had discovered malicious files in the wild in Japan that attempt to exploit the **Excel Unspecified Remote Code Execution Vulnerability**.

The patch affects **Microsoft Office**, 2002, 2003, and 2007, as well as **Microsoft Office** 2004 and 2008 for the **Mac**, according to the **Microsoft bulletin**.

Microsoft also released a patch for a critical vulnerability in WordPad and Office that could allow remote code execution if a specially crafted file is opened in WordPad or Microsoft Word. This vulnerability is currently being exploited on the Internet, Microsoft said. It affects Windows 2000, Windows XP, Windows XP Professional, Windows Server 2003, Microsoft Office Word 2000 and Word 2002.

Another patch fixes four critical vulnerabilities in Internet Explorer that could allow remote code execution if a user views a specially crafted Web page or if a user connects to an attacker's server via HTTP. Exploit code and attack details have been made public for a couple of the vulnerabilities. Affected software is IE 5, 6, and 7.

A patch for Microsoft DirectShow closes a critical vulnerability that could allow an attacker to take complete control of a system if a user opened a specially crafted MJPEG file. It affects DirectX 8 and DirectX 9.

A fifth patch addresses critical vulnerabilities in Windows HTTP services that could allow an attacker to take complete control of the system and for which exploit tools and code have been made public. Affected are Windows 2000, Windows XP, Windows XP Professional, **Windows Vista**, Windows Server 2003, and Server 2008.

Also fixed are important holes in Windows being exploited in the wild that could allow elevation of privilege if an attacker is allowed to log on to a system and run a specially crafted application. Windows 2000, Windows XP, Windows XP Professional, Windows Vista, Windows Server 2003, and Server 2008 are affected.

Other patches address less critical holes in Microsoft Internet Security and Acceleration Server 2004 and 2006 and the medium business edition of Forefront Threat Management Gate, as well as SearchPath. Attack details have been made public for the SearchPath blended threat vulnerability. It affects Windows 2000, Windows XP, Windows XP Professional, Windows Vista, Windows Server 2003, and 2008.

In all, Microsoft issued eight patches for about two dozen reported vulnerabilities.

"We were astonished to see how many zero-days are in that release," said Wolfgang Kandek, chief technology officer of Qualys, in reference to exploits that target software with a vulnerability that has not been patched yet.

"Ten of the vulnerabilities have either exploits out in the wild or there is proof-of-concept code available and that's a first, I think, in terms of the number of zero days in a single bulletin," he said. "For the IT guys, that means their window has just shrunk to zero to get these things fixed."

The IE vulnerability is of particular concern, Ben Greenbaum, senior research manager at Symantec Security Response, said in an e-mail statement. It "appears to be the easiest of the bunch to take advantage of by an attacker and also happens to be the one that requires the least amount of involvement by a user to exploit. An attacker can simply lure a victim into viewing a Web page that contains malicious content and that

individual's computer can then be taken over."

Missing from the bulletin was a fix for a zero-day hole in PowerPoint that Microsoft **warned on April 2** had been targeted by attackers.

In honor of Patch Tuesday, Check Point Software technologies said it was selling a full version of its ZoneAlarm Internet Security Suite for $9.95 instead of $49.95. The sale runs for 24 hours starting at 6 a.m. PDT on Tuesday. Check Point said it will donate half of the proceeds to non-profit TechSoup Global.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Vulnerabilities & attacks**

Tags: **Microsoft**, **Windows**, **Patch Tuesday**, **Excel**, **Word**, **exploit**

Related

From CNET

Microsoft seeks Windows Mobile update leader

Latest Windows ads parodied in Web video

Microsoft to patch Excel hole, seven others

From around the web

Microsoft Plans Three Security Bulletins... eWeek

Microsoft Plugs Eight Windows Security H... Washington Post Blogs - Securi...