Microsoft probing new hole in IE security

February 3 2010

Attendees try an interactive display at the Microsoft booth at the 2010 International Consumer Electronics Show, in January 2010 in Las Vegas, Nevada. Fresh from patching an Internet Explorer (IE) flaw exploited in cyberattacks on Google and other firms, Microsoft is looking into a newly exposed vulnerability in the browser software.

Fresh from patching an Internet Explorer (IE) flaw exploited in cyberattacks on Google and other firms, Microsoft is looking into a newly exposed vulnerability in the browser software.

"Microsoft is investigating a responsibly disclosed vulnerability in Internet Explorer," Microsoft Trustworthy Computing group manager Dave Forstrom told AFP on Wednesday.

"We're currently unaware of any attacks trying to use the vulnerability or of customer impact, and believe customers are at reduced risk due to responsible disclosure."

The IE flaw is unrelated to cyberattacks disclosed by Google and only poses a threat to computers running on the US software giant's Windows XP computer operating system, according to Microsoft.

A computer defense firm that alerted Microsoft to the IE flaw presented "proof-of-concept" code Wednesday at a Black Hat technology security conference in Washington, D.C.

The demonstration revealed "an information disclosure vulnerability" in IE browsers run on XP or other operating systems if IE Protected Mode is disabled, according to senior security communications manager Jerry Bryant.

"People running IE 7 or 8 in default configurations on Windows Vista or later operating systems are not vulnerable to this issue as they benefit from Protected Mode," said Bryant.

The software giant issued a security advisory warning of the danger and recommending XP users enable a "Network Protocol Lockdown" feature and IE software be set to "Protected Mode."

Users were advised to upgrade to Microsoft's new Windows 7 operating system and the latest browser, IE 8, which feature significant safeguards against hackers.

"Once we're done investigating, we will take appropriate action to help protect customers," Forstrom said.

"This may include providing a security update through the monthly release process, an out-of-cycle update or additional guidance to help customers protect themselves."

Microsoft only veers from its usual protocol of releasing security updates

the second Tuesday of each month when it deems fixes urgent.

Two weeks ago, Microsoft released an out-of-cycle patch for an IE 6 software hole through which China-based cyber spies attacked Google and other firms.

Microsoft has confirmed that the previously unknown security vulnerability in its IE 6 browser was used in cyberattacks which prompted Google to threaten to shut down its operations in China.

Revealing the attacks on January 12, Google said they originated from China and targeted the email accounts of Chinese human rights activists around the world. The company did not explicitly accuse the Chinese government of responsibility.

Web security firm McAfee Inc. said that the attacks on Google and other companies showed a level of sophistication beyond that of cyber criminals and more typical of a nation-state.

Attackers used email or some other lure to get employees of a targeted company to click on a link and visit a specially crafted website using Internet Explorer.

Malicious software would then be downloaded that has the capability to essentially install "back doors" in machines and give hackers access.

(c) 2010 AFP