

Microsoft plans to patch critical Windows bug the week of 1/13/2011

But it's not ready to fix newest IE and Windows flaws By Gregg Keizer, January 6, 2011 02:57 PM ET

Microsoft today announced it would release just two security updates next week to patch three vulnerabilities in Windows on 1/11/2011. (I received 8 for Vista 64 bit - Carole)

One is "critical" while the other was marked "important." Microsoft typically assigns a critical rating to vulnerabilities that can be exploited with little or no action on the part of a user.

Both updates will patch flaws in Windows.

What Microsoft pegged as "Bulletin 1" in the [advance notification](#) it published today will affect only Windows Vista, while "Bulletin 2" will affect all still-supported versions of the OS, with the client editions -- XP, Vista and Windows 7 -- labeled critical and the server software rated important.

"The Vista one is confusing," said Andrew Storms, director of security operations at nCircle Security. "It's either something introduced in Vista but doesn't exist in Windows 7, or the component was rewritten for Windows 7." Storms speculated that the flaw might be in a part of operating system that's little used, such as the task scheduler.

As for Bulletin 2, Microsoft's bare bones write-up -- typical of its advance warnings prior to Patch Tuesday -- also doesn't offer many clues.

"It's critical in all the desktop clients and important in the server, and consistent in the whole stack," said Storms, talking about Microsoft's threat ratings. "The difference in the criticality is confusing, and Microsoft's not giving us much to go on."

The bug(s) patched by Bulletin 2 are most likely in an operating system DLL (dynamic-link library), said Storms, perhaps a driver or database connector, that's crucial to the OS.

Microsoft will not be patching either of the vulnerabilities that the company recently acknowledged -- and issued security advisories for -- said Carlene Chmaj, a spokeswoman for the Microsoft Security Response Center (MSRC), in a post Thursday to the [team's blog](#). "We continue to actively monitor both vulnerabilities," she said.

Two weeks ago, Microsoft [confirmed a critical bug](#) in all versions of IE, including the newest production edition IE8, that hackers could exploit by convincing users to visit a malicious site. On Tuesday, the company [acknowledged a serious flaw](#) in Windows XP, Vista, Server 2003 and Server 2008.

Microsoft has seen in-the-wild targeted attacks exploiting the IE bug. Microsoft typically releases an emergency, or "out-of-band," security update only if attacks spike. Nonetheless, some researchers were surprised that Microsoft isn't addressing the two bugs next week.

"The big shock this month is that Microsoft is *not* addressing two security advisories that have already been weaponized," .

"The only chance that they would have patched [the two outstanding bugs] is if they already knew about them months before,". "If anyone is surprised that [those bugs] are not being patched, they don't follow Microsoft's release cycles very closely."

It's possible that Microsoft may be forced to release an IE update a week or two early. That update, expected Feb. 8, would conceivably include not only a fix for the bug Microsoft confirmed Dec. 22, but also one for the vulnerability Google security engineer Michal Zalewski [told Microsoft about](#) last July.

Abraham anticipates an early IE update. "I would bet that if the malicious attackers start using the [public] exploits then we will see an out-of-band patch," he said.