Security patch results in BSOD, stops Windows from booting

By Emil Protalinski | Last updated February 11, 2010 11:43 AM

One of the updates from this month's giant Patch Tuesday is wreaking havoc on some users Windows PCs by giving them the Blue Screen of Death (BSOD), according to a thread on Microsoft Answers, the company's support forum. Based on what users have found, the update in question is KB977165, which is described by Microsoft as "MS10-015: Vulnerabilities in Windows kernel could allow elevation of privilege" (for those wondering, yes this is the 17-year-old Windows flaw we reported about last month). The issue was first reported by Krebs on Security.

Microsoft Security Bulletin MS10-015 goes into further detail about the flaw being patched: "The vulnerabilities could allow elevation of privilege if an attacker logged on to the system and then ran a specially crafted application. To exploit either vulnerability, an attacker must have valid logon credentials and be able to log on locally. The vulnerabilities could not be exploited remotely or by anonymous users." The security update is rated Important on the versions of Windows it patches: Windows 2000, Windows XP (32-bit and 64-bit), Windows Server 2003 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit), and Windows 7 (32-bit).

The majority of users who are complaining about the issue are on Windows XP, but some users in the thread mention this occurs for them on Windows Server 2003 and Windows Vista. Those running Windows 2000, Windows Server 2008, and Windows 7 have yet to report problems (edit: we now have confirmation of this BSOD occurring on Windows 7, see this thread on Microsoft Answers), though the issue is fairly new so it's still possible that as more and more users install the update, the BSOD will creep up on the remaining versions of Windows as well. We have yet to see the problem occur, as most of our systems and those of our peers are running Windows 7 64-bit or Windows Server 2008 R2.

The thread starter explains the problem at hand: "I updated 11 windows xp updates today from Microsoft.com and restarted my pc like it asked me to. (There has definitely been absolutely NO CHANGE in my computer software or hardware installation apart from [these] updates) From then on, Windows [could not] restart again! It is stopping at the blue screen with the following message:

> A problem has been detected and windows has been shutdown to prevent damage to your computer.
>
> PAGE_FAULT_IN_NONPAGED_AREA Technical Information: STOP: 0x00000050 (0x80097004, 0x00000001, 0x80515103, 0x00000000).

"I tried all kinds of restarting option[s], namely safe modes etc. but everything is returning to the blue screen," he concluded. Another user wrote: "Samething [sic] happened to me. I think there is something seriously wrong with the update. I can't even open in safe mode..."

Users in the thread have tracked down a fix, though it requires using a copy of the Windows disc (or for netbook users without an optical drive, a bootable USB drive with Windows on it):

1. Boot from your Windows XP CD or DVD and start the recovery console (see KB307654 for help with this step)
2. Type this command: CHDIR $NtUninstallKB977165 $\spuninst
3. Type this command: BATCH spuninst.txt
4. Type this command: systemroot
5. When complete, type this command: exit

This fix has been marked as the answer to the thread by Cody, a Microsoft Support Engineer. Formally, the suggestion actually says to repeat steps two through four with all the following patches: KB978262, KB971468, KB978037, KB975713, KB978251, KB978706, KB977165, KB975560, and KB977914. Since that post, users have concluded in the thread that KB977165 is the problematic update.

Robear Dyer, a Microsoft MVP, gave three pointers to users in the thread:

1. Uninstalling KB977165 will automatically restore the previous versions of ntkrnlpa.exe and ntoskrnl.exe so there's no need to find "a way to replace them."
2. That being said, the newer versions of ntkrnlpa.exe and ntoskrnl.exe address the very serious and currently -being-exploited security vulnerability described in MS10-015, so you really do not want to avoid this update! Instead, open a free support incident per my previous reply.
3. Encountering a STOP error (e.g., 0x00000050) after installing this update could mean that your computer's already been compromised by the security vulnerability addressed by MS10-015, yet another reason to open a free support incident!

The only problem with these suggestions is that most users can't boot their computer to uninstall the update (both "Last Known Good Configuration" and Safe Mode don't work). While the solution most users have found to work is to boot off the Windows XP disc and use the Recovery Console, Dyer is suggesting finding some other means to uninstall the update. Users are naturally more interested in getting their computer functioning again than making sure it is secure.

"Microsoft is investigating reports of an installation issue with a security update released on February 9, 2010," a Microsoft spokesperson told Ars. "We are investigating the issue to determine the cause of the issue. Anyone believed to have been affected can visit: consumersecuritysupport.microsoft.com. Those in the United States can contact Customer Service and Support at no charge using the PC Safety hotline at 1-866-727-2338 (PCSAFETY). Those outside the United States can find local contact numbers at support.microsoft.com/international." The company has since pulled the patch from Windows Update.

Further reading

- Restart issues after installing MS10-015 (blogs.technet.com)
- Update - Restart Issues After Installing MS10-015 (blogs.technet.com)