

Re: Missing Windows update reported as a vulnerability by TMH and

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2007-10/msg01083.html>

- *From:* "MowGreen [MVP]" <mowgreen@xxxxxxxxxxxxxx>
 - *Date:* Sun, 28 Oct 2007 15:22:28 -0700
-

I believe that for most of the times, SDHelper was blocking malware content coming not directly from the site itself, but instead from some third party advertising company which was displaying ads in that site.

It was blocking Cookies, not malware. You can easily do that by adding the sites to a Host file, or, use this Host file:

<http://www.mvps.org/winhelp2002/hosts.htm>

Don't use Belarc as the 'bible'. The way to determine that KB939653 is installed properly is to have the system scanned at either Windows or Microsoft update and then go over the Security bulletin to ensure that the files are at their correct Versions and that the registry shows that the update has been applied successfully.

MowGreen [MVP 2003-2008]

```
=====
*-343-* FDNY
Never Forgotten
=====
```

Hugo_Pt wrote:

This time i did things differently, and followed the latest MowGreen recommendation. I ended up with only KB939653 listed under Windows Internet Explorer 7 Software Updates in my 'Add or Remove programs' instead of both KB939653 and KB938127. However KB938127-IE7 is listed in Belarc's report under 'Installed Microsoft Hotfixes', so i guess it is just "hidden" in my 'Add or Remove programs'. On the other hand, Belarc A. still reports KB939653-IE7 as a *missing* update. It still appears under 'Missing Microsoft Security Hotfixes' in Belarc's report.

Steps done:

Step 1. I disabled Windows automatic updates, and also disabled Avast, Windows Defender real time protection, and even "SDHelper"(although it probably wasn't necessary). No need to disable "TeaTimer" since i always have it disabled.

Re: Missing Windows update reported as a vulnerability by TMH and

Step 2. I uninstalled IE7, without previously uninstalling any IE7 update. After reboot, i checked 'Add or Remove programs'. Both IE7 and all the IE7 updates (2 updates) were not listed.

Step 3. I disabled again Avast resident protection, since after reboot it was automatically re-enabled. I installed IE7. This time, i didn't put a checkmark in the checkbox asking to download the latest IE7 updates and the malware removal tool during IE7 installation.

Step 4. I reboot twice. Then re-enabled Automatic Updates (configured it to automatically download updates but to not install them without asking me first). AU downloaded just the KB939653 update for IE7. I disabled Avast once more, and installed the downloaded update. Reboot.

Step 5. I ran Belarc A.. Once more, it failed verification of KB939653-IE7.

Step 6. I disabled again AU. I uninstalled KB939653, rebooted, and disabled Avast. Then installed manually the KB939653 for IE7, by running 'IE7-WindowsXP-KB939653-x86-PTG.exe' which i had stored before in my HD.

Step 7. Reboot and reconfigured AU to notify me about any existing updates, but to only transfer and install them after i tell to. This is my usual AU configuration. Then, ran again Belarc A. Same disappointing result... >:-(Perhaps a 'false positive' ? No way to know for sure.

No more steps !

It's curious that from 3 or 4 IE7 updates listed in 'Add or Remove programs', i passed to 2, and now, from 2, i passed to just one.

Mowgreen: You say that SDHelper is totally useless, but you don't explain why. To me, it's been useful, IMHO. For instance, it alerted me that Spybot blocked '/Avenue A, Inc.' or 'Doubleclick' when i was entering certain sites, including when going to sites that i considered "safe", such as www.download.com. I believe that for most of the times, SDHelper was blocking malware content coming not directly from the site itself, but instead from some third party advertising company which was displaying ads in that site. But nevertheless, i consider it is useful to be warned whenever malware-delivering URLs (third party or not) are stopped from dumping trash in my PC. Just my opinion (JMO).

As english is not my language, i don't know what the expression 'Your mileage may vary' means. I checked 'mileage' in one online english dictionary, but it makes no sense ;)

"MowGreen [MVP]" wrote:

This is where 'problems' arise :

Step 3. I downloaded and reinstalled Internet Explorer 7.
During IE7 installation, I was given the option to download

Re: Missing Windows update reported as a vulnerability by TMH and

and install immediately any IE7 updates along with the IE7 installation (the same checkbox allowed also to download and run immediately the Microsoft latest malware removal tool). I ticked that checkbox, and started the installation, but at the end of the process, i was told that not all the IE7 updates were successfully installed, and that i should reboot my computer, then open Internet Explorer and go to the 'Windows Update' site to install any remainder updates.

During the installlation of IE7 it is HIGHLY recommended that one disable Automatic Updates :

http://www.ie-vista.com/known_issues.html#pre-install

If one allows Automatic Updates during the install of IE7 that means that files that are being written to the HardDrive are being replaced by files downloaded from AU either while they're being written or right afterwards. Not good practice, IMHO.

Just allow the files to be written and then reenable AU.

Thanks for posting the Version of jscript.dll that is installed with IE7. It's too bad that Microsoft hasn't published a file list as they did for previous versions of IE.

Now, as to Spybot ... although it's not active it can/will cause issues when TeaTimer is enabled when updates are installed.

Disable TeaTimer either right before updating or all together.

Said issues can/will occur when the system is installing updates from either of the Update sites, not when using Automatic Updates.

That's because TeaTimer monitors/blocks ActiveX components and the Update sites use that component [wuweb.dll for Windows Update; muweb.dll for Microsfot Update] during the updating process.

SDHelper is totally useless, IMO. Your mileage may vary [YMMV ;)]

MowGreen [MVP 2003-2008]

=====

-343- FDNY

Never Forgotten

=====

Hugo_Pt wrote:

Mowgreen:

Besides Avast, i have also Spybot-S&D, Ad-Aware 2007 (Free Edition), SpywareBlaster and Windows Defender installed, but from these 4, only Windows Defender has real

Re: Missing Windows update reported as a vulnerability by TMH and

time protection monitoring my system in the background. Spybot-S&D has two additional resident protection modules: Resident "SDHelper" and Resident "TeaTimer". "SDHelper" is an Internet explorer bad download blocker. It is an IE add-on (Browser Helper Object) that blocks any content coming from a list of known malware sites when i'm browsing the web. I always have it enabled. "TeaTimer" protects over-all system settings. I never activated it. I also have Peerguardian 2. It blocks IPs from selected lists. Most of the time i only have the 'Spyware' list of IPs enabled. PG2 works at the kernel level (don't know what this means).

Yesterday, I couldn't wait for MowGreen's reply. My browser stop responding for 2 times, when closing IE7 window, and I felt an urge to solve this without more delays. So, I did the following:

Step 1. I had at least 4 IE7 updates listed in 'Add or Remove programs'. I didn't know if i should uninstall them all before uninstalling IE7, or if I should uninstall only IE7, hoping all the IE7 updates to be automatically uninstalled in the process. I uninstalled only the KB939653, then I uninstalled IE7.

Step 2. After uninstalling IE7, i noted that KB917344 appeared in my 'Add and Remove programs' (it was hidden before by IE7) and also noted that jscript.dll on WINDOWS\system32 was now v.5.6.0.8831. Also, after uninstalling IE7, one last IE7 update remained in the 'Add or Remove programs'. I chose to remove it, and clicked on 'Continue' when an *annoying* dialog box showed up, warning me about a list of programs *and Windows updates* that might not work correctly if that update was removed.

Step 3. I downloaded and reinstalled Internet Explorer 7. During IE7 installation, I was given the option to download and install immediately any IE7 updates along with the IE7 installation (the same checkbox allowed also to download and run immediately the Microsoft latest malware removal tool). I ticked that checkbox, and started the installation, but at the end of the process, i was told that not all the IE7 updates were successfully installed, and that i should reboot my computer, then open Internet Explorer and go to the 'Windows Update' site to install any remainder updates.

Step 4. The first thing i did after reboot was to check jscript.dll version. It was Version 5.7.0.5730 !! "mae" was right... I also checked 'Add or Remove programs': Under Windows Internet Explorer 7 Software Updates , the only IE7

Re: Missing Windows update reported as a vulnerability by TMH and

update listed was KB939653. Then, i went to 'Microsoft Update' site. It found only one IE7 update missing: KB938127. I downloaded and installed it.

I think it's curious that before *Step 1.* i had 4 IE7 updates listed in 'Add or Remove programs', and now i'm reduced to only 2.

Step 5. I reinstalled Belarc Advisor and ran it. Now, it no longer detects KB917344 as a missing update –*one problem less*–, but it still detects KB939653–IE7 as missing:

« Missing Microsoft Security Hotfixes
KB939653–IE7 – Critical (details...) These required security hotfixes (using the 10/09/2007 Microsoft Security Bulletin Summary) were not found installed. Note: CIS benchmarks require that Critical and Important severity security hotfixes must be installed.»

Step 6. I uninstalled KB939653 and reinstalled it (via automatic updates). Then, ran Belarc A. again, but it still failed verification of KB939653–IE7.

Have I done something wrong through steps 1–5 ? Or Belarc reported a 'false positive'? I'd like to know the answer. Any suggestions ?

Two more notes:

Note 1. In *Step 3.* , before downloading IE7, I went to 'Microsoft Update' site, and it prompted me to install missing KB939653 for IE6. I didn't download it, as i was going to install IE7.

Note 2. Before installing IE7 and IE7 updates, i disabled both Avast and Windows Defender.