

MS03-026 – are you patched? Windows Update isn't sure!

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0075.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 07/30/03

Date: Wed, 30 Jul 2003 17:42:40 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

FYI, it is worth reminding people that some patch checking tools don't do a complete check. Windows Update doesn't check files, and it would seem that other products have problems also.

Some tools only check for the presence of a registry key indicating that a hotfix was applied. Other tools, such as Shavlik's HFNetchk and MBSA (and others) actually check file details, including a checksum, to verify that the files in play are actually the right versions.

I was speaking with Jeff.t.Parker @ hp.com about this issue. His observations confirm this (see below). If patched files are reverted to previous versions, for whatever reason, Windows Update and (at least in this case) Update Expert (and possibly other such tools) will incorrectly assert you have the patch applied when in fact you don't.

He wrote in to advise that Update Expert (v6.0 build 6069) is giving erroneous results at least in some cases. After applying SP4 concurrently with MS03-026 (using Update Expert), Jeff noticed some interesting results. The resulting versions of the files contained in MS03-026 on some machines were;

5.0.2195.6692 ole32.dll
5.0.2195.6701 rpcrt4.dll
5.0.2195.6702 rpss.dll

This led to Windows Update and Update Expert both reporting that the systems had MS03-026 applied (wrong). MBSA and eEye's Retina both said the systems *did not* have MS03-026 applied (right).

While this may be a problem with the way Update Expert deploys Service Pack + Hotfix combinations, it also demonstrates the problem Windows Update has by not being able to examine file details (relying only on registry entries).

How many systems are out there now who believe they have MS03-026 applied, can't get it offered to them from Windows Update, but in fact don't have it applied at all??

Cheers,
Russ – NTBugtraq Editor

oo
Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!

