

Delving into the contents of MS03-026 on XP

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-08/0043.html>

From: GDWNet Security (*Security_at_GDWNET.COM*)

Date: 08/13/03

Date: Wed, 13 Aug 2003 00:58:43 +0100
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

I'm just in the process of putting together some notes about the MS03-026 patch process in light of the blaster worm and have been taking a much closer look at the XP patch.

If you run the XP patch followed by a -x to extract the contents to a directory you will see that there are three folders, common, sp1 and sp2. In the SP1 and SP2 folders are separate copies of the ole32.dll, rpctr4.dll and rpcss.dll files with different version numbers. Those in the SP1 folder have a version number of 5.1.2600.115 and those in SP2 have a version number of 5.1.2600.1243

Maybe I'm missing something here but I don't understand why there are two different sets of 'fixed' files and why they have different version numbers.

I've installed the patch on a test SP1a platform and verified via the MD5 hashes that the files from the SP2 directory have been installed.

I've not yet installed a 'clean' build of XP to see what version of the files get installed by this patch nor have I looked at Software Update Services to see what version(s) of the patch it has but I don't understand why Microsoft feel it necessary to have two different versions of the fix for XP.

--
Gary Williams.
security@gdwnet.com
oo
Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!
With a growth rate exceeding 110%, the TICSAs security practitioner
certification is one of the hottest IT credentials available. And now, for
a limited time, you can save 33% off of the TICSAs certification exam! To
learn more about the TICSAs certification, and to register as a TICSAs
candidate online, just go to
<http://www.trusecure.com/offer/s0100/>
oo