

Re: Conflicting info between the global Security Bulletin and some SPi Security Bulletin

Re: Conflicting info between the global Security Bulletin and some SPi Security Bulletin

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2007-02/msg00070.html>

- *From:* "David F" <David-White@xxxxxxxxxxxxx>
 - *Date:* Sat, 24 Feb 2007 23:27:20 -0800
-

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message news:egH2vBEWHHA.3568@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"David F" <David-White@xxxxxxxxxxxxx> wrote in message news:u2wGns9VHHA.4796@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

The global detailed Security Bulletin is given in:
<http://www.microsoft.com/technet/security/current.aspx>

I did find the following problems there.

I normally use Win 2K + SP4.

According the Security Bulletin for the release of SP4,

(<http://www.microsoft.com/technet/security/prodtech/windows2000/w2ksp4.msp>)

it contains all new (new – with respect to SP3) patches in the range:

MS01–022 (4.18.2001) till MS03–030 (7.23.2003)

and of course also all prior patches from SP1 to SP3.

But when I looked in that detailed global list, I find for example that as old

MS00–077 (10.13.2000 !) and many other older than MS03–030 should be applied to W2K/SP4. This doesn't make sense.

I do not see statement that ms00–077 applies to W2k Sp4

Where do you see this? In what you term the Global Sec Bulletin it

states this applies to W2k at Sp1 and Sp2, and if you read into it you

will see that the Sp2 part was added when the specific patch was

reissued to address a further, similar exploit. If you look at the KB

<http://support.microsoft.com/?kbid=299796>

you will see that the updated patch was first included in SP3

You are right – I copy and paste the wrong patch #. I meant to specify MS02–032 dated: 6.26.2002, which is listed specifically as already included in the SP4.

Re: Conflicting info between the global Security Bulletin and some SPi Security Bulletin

I found the exact same contradictions with regard to Win XP SP2. In this case, I found even a worse situation, when patch # MS03-011 showing up in the detailed global list, which according to its date and patch # should be included in the Security Bulletin list for WXP/SP2 but it is not!. This list is given in:
<http://www.microsoft.com/technet/security/prodtech/windowsXP/xpsp2.msp>

ms03-011 is something of a peculiar situation as it deals with the MS distributed Java VM, which MS had to pull from availability as part of a settlement with Sun. In fact, this was involved in the reissue of XP Sp1 as XP Sp1a. It is possible for even W2k3 to need this patch. It all depends on

I am confused by "...possible...". This one is ranked "critical" for installing explicitly on W2K3 (as a matter of fact, on W2K2/3/4). But then again, like MS02-032, it should have already been included in W2K4. But again, what is worst, in spite of being released before SP4 was released, I would expect it to be included in SP4 and me NOT needed to install it on a W2K4. And like with WXP, it is missing from the Security Bulletin list for SP4.

the history of the machine. One could install an XP SP2 from an XP Sp2 CD and not get the VM installed. Later, install of an older download of some product might install the VM at a level before 3810, causing need for the patch at that point. Read into the bulletin and you will see there is quite a bit that is abnormal about this specific patch. Behind the scenes there is a bit of legal history. One must take the history of a specific machine into account to determine need, and just being at an OS level mentioned in the bulletin does not mean one needs the patch (the VM might not be present).

I am confused from the explanation.

My key point is that when I install a new system, I am obviously expected to install the highest SPi (and for WXP I do have and use indeed the XP SP2 CD you mentioned to install XP) and then simply add (manually in my case) each patch listed in that global list that was released after the release of that SPi, and that that list explicitly says it applies to that SPi.

It is that simply and that straight forward.

Accordingly, I would not expect any patch listed as released before the release of a specific SPi, being mentioned as still applicable for that SPi.

Re: Conflicting info between the global Security Bulletin and some SPi Security Bulletin

And in the case of W2K, we have something called Rollup_1_ver_2—for SP4 which is even higher than SP4 (and I did not see an explicit list of what security patches it contains) and it is not mentioned in that global list. So the only way I can relate to it is by relating to the date of the last patch included as mentioned in its release notes. So I would use any patch listed in the global list as mentioned above but that its release date is not just higher than the last one to be included in SP4 but higher than that last date of that Rollup.

BTW, I also would think that it should not matter, that for the case of XP, for example, that it would not matter whether one installs the very original XP he has and add later the downloadable SP2 or use that CD mentioned above.

So I don't know what to make of it and how I can rely on that detailed global list in terms of what to pickup from it and apply to W2K/SP4 (and the same for WXP/SP2).

You seem to be going about this the hard way David.
You can either use the Microsoft Update site in Custom mode to get a list of what a specific machine needs based on what is at the moment installed; or one can download MBSA and after it is installed open a cmd prompt at the install directory and issue `mbsacli /?` for syntax, and then use `mbsacli` with a switch `/n OS+IIS+SQL+Password` in order to only check patches

You are right about "the hard way" – to some degree. But – when I looked once into that MBSA "thing", it looks to me overly cumbersome (like most other things from MS) and also things being changed all the time. So I am not sure if in this case it is worth the time invested in it. I might be wrong of course.

My understanding is that there is something called a "scan file" which is something like a definition file (like for viruses detection for example), that the executable MBSA program uses to figure out what my SW product(s) already have and produces a list of MS0X-0YYs (or similar) I do need still to install. And, if the executable and "scan file" are installed, it is all done offline.

It seems that for Office 2K I still have to use MBSA ver. 1.2.1. But I could NOT find an offline scan file for that ver. and my impression is that this version works online only – exactly the kind of things I am trying to avoid. Even for MBSA ver 2.0.1, I could not find the scan file, especially the new one.

Re: Conflicting info between the global Security Bulletin and some SPi Security Bulletin

David

=====

Albert Einstein: "Everything should be made as simple as possible, but not simpler."

.