

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/msg00075.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Mon, 26 Feb 2007 08:04:41 -0700
-

I really do not know how best to respond to you expect to say that if it is called out as affected (note that this does not always mean needed, just that it can be needed) then there is/are case(s) in which it can be needed.

I have every reason to believe the folks at MSRC know what they are doing this regard, having been in on email exchanges previously (nearly monthly) about making sure the released bulletins are clear and accurate.

Also, keep in mind that it was only somewhere around the end of 2002 when the patch updater technology started to see the results from the push for improved strategy and for unification of the multiple updaters in use. Prior to that time it was possible to have a patch not take just because it was applied in the wrong order while applying a specific group of reboot requiring patches at the same time without reboots.

Anyway, the scanning tools are the best way to determine what is needed by the current state of a system. Yes, this does get more difficult for a non-connected system, and yes, for older, end-of-life products one may have to use a variety of tools to scan as much as possible. Nevertheless, trying to wind one's way through the fine details would really mean looking at the installed binaries on the system and comparing their versions with the versions called out as supplied by the patches (in the bulletin or associated KB). One cannot just say, this is a W2k at SP 4, and since the high-level statement of affected versions includes that OS therefore this one needs this. If you really want to do the decision process you might need to read into the cab files used in the scans and look at just what detection info they are keying in on, which you will find in the xml called out per OS version.

For the VM example you say, well yes that particular install history would result in a vulnerable system, but it is that person's fault that they did that. That may be true enough,

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

but you know where that person will place the blame, right?

There used to be a number of pages on the web that tracked the patches, trying to organize the info much as you seem to be attempting. As far as I know, those people have mostly all stopped keeping their listings updated subsequent to the release by MS of the scanners. There is a reason, it is just hard to do better than one gets by running a scan.

Roger

"David F" <David-White@xxxxxxxxxxxxxx> wrote in message
news:%232B3deXWHHA.480@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message
news:us3yDJPWHHA.1180@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

"David F" <David-White@xxxxxxxxxxxxxx> wrote in message
news:O2aGr5KWHHA.4844@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

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

The global detailed Security
Bulleting 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.r>
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.

That is a Windows Media Player (WMP) patch.
Tell me, what happens in the following scenario . . .
Someone has W2k with WMP 6.4 (which I think is what came with W2k),
and they install SP 4 when it come out.
Then they elect to upgrade to WMP 7.1, but they use a download of the
WMP 7.1 installable obtained before the download was updated to have
the patch of MS02-032 included within it.
So, they have a W2k at SP4 with a vulnerable version of WMP 7.1, no?

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

I think the answer is NO – if one behaves reasonably. And here is my rational.

If the downloaded WMP 7.1 is from before the release of MS02–032, then when SP4 would come out and installed, the WMP would be updated.

If the WMP 7.1 was downloaded after the release of MS02–032, whether before the release of SP4 OR EVEN AFTER the release of SP4, then the WMP should incl. it and the release and installation of SP4 should have no impact (as far as MS02–032 is concerned).

If there was no updated version of WMP7.1 after MS02–032 release (and actually even if there was), it is OK for the global list to say that it is applicable to such and such version or release date or file date of WMP7.1.

Either way, there is no point to say in the global list that MS02–032 applies to W2K4 because it is not.

Of course, if one downloaded WMP7.1 before MS02–032 released, kept it in the drawer, then downloads and installs SP4, AND ONLY THEN decided to install that OLD WMP7.1 then it should be HIS problem – stupidity is indeed costly. It is reasonable to expect that when one installs something, s/he would use the most recently available version and/or in proper order.

I thought that this is an ABC and elementary logic. Isn't it?

You tell me, am I missing something? Did I leave any scenario uncovered?

But wait, there is more.[J]

MS02–032 was just an example. There are 4 more mentioned in the global list as applicable to W2K4: MS03–026, MS03–023, MS03–022 & MS02–050 – ALL within the period of time that SP4 is suppose to cover. The first 3 (MS03–.) though are NOT listed as included in the SP4 release (see my link above) although they belong there by date according release notes

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

for SP4. MS02-050 (like MS02-032) IS explicitly incl. in the SP4 release, and unlike MS02-032, it doesn't pertain to some add-on such as the WMP but purely to the core OS. And there is even more to this MS02-050 patch. It even shows up in the list of patches included with Rollup_1(V2) for SP4 (hereafter R1V2). Now the release notes for R1V2 say clearly that SP4 must be installed first.

My hunch is that I should not install patches such as MS02-050 on top of SP4 (let alone on top of R1V2) but what say you in this case?

And what should I make about the other 3? I have no clue whether I should go ahead and add them on top of SP4 or not (and again, let alone on top of R1V2). They are listed in the R1V2's list of patches.

See: <http://support.microsoft.com/kb/891861>

Luckily, nothing in the global list references the R1V2.

All in all, I am in square one of my original thread. I would obviously start with manual installation of individual patches after installing R1V2 and again the question is whether it is OK to go by date (in order of course), that is, to pickup from the global list all patches dated after the last patch included in R1V2's list and ignore anything else.

In general, I agree with you that there could be, for historical, legal, and other reasons some peculiar scenarios but this doesn't mean that the "Affected Software Service Packs" column, like any other piece of technical info should not be precise and unequivocal stated.

You are attempting to make thing too clear-cut; that way does not match the realities encountered in world.

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.mspx>

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,

W2k4 ?

Yes.

Look. At a fixed point in time MS took away from the web all downloads that included an install of the MS Java VM. This was required by the Sun lawsuit settlement. That does not mean that people could not use things

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

obtained before that time to cause it to install.

Hence, it is known that the VM might be installed on certain versions, that it certainly is installed on some or via specific built histories, etc..

But, of those, only some can have the statement "the VM is installed" made with certainty. Hence, how can you expect them to say the patch is needed with certainty?

You will not find the VM on a fresh W2k3 install nor after SP1. Yet W2k3 is called out in this bulletin. Why? Because some histories leading to that instance of a W2k3 build could have caused the VM to become installed.

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

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

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.

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.

Take the case of the VM patch.

To meet the court mandate MS removed all downloadables the would install the VM. This included purging the MSDN downloads for subscribers of W2k with SP4 inlined CD image, etc.

They also released IIRC version 3810 of the VM, which would install only if the VM was already present on the machine.

Prior to 3810 the VM distributions would update an existing VM if present or install the VM if not.

Many people wanted to not use the Sun JRE, so you will find even today downloads of the VM that will install when the VM is not present, provided only that it is a support OS. So, people can build a XP SP2, which today will be without the VM, and then apply one of these older VM distributions (obtained from third-party archives) and it will install and it will leave the machine at a vulnerable VM version if they omit downloading and applying the 3810 VM update.

So, can XP SP2 be in a state that needs the patch? Yes.

Would a XP SP2 installed from a XP SP2 CD need it? No.

Would an XP installed from the original gold XP CD need it? Yes.

Would a gold XP install with SP 2 applied need it? No

Could a gold XP plus SP2 be caused to need it? Perhaps, likely not. (one could uninstall 3810 and then use outdated download . . .)

Things are just not as clear-cut as you would like.

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

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

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.

If you cannot see the simplicity of mbsacli usage I do not know
how you could be convinced, nor do I wish to try.

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

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

works online only – exactly the kind of things I am trying to avoid

I believe you are correct, that only the old MBSA will detect for O2k
<http://support.microsoft.com/kb/895660/en-us>
But, IIRC MS will stop providing scan files in the old form as of March, whence only ver 2.x releases of MBSA will be supported.
Also, is not O2k beyond its service lifetime? so one would not expect to see further patches soon (like W2k which will soon no longer have even security patches released to the public).

That is OK. I never referred to future expectations but only to what has been released in the past. And actually, MS promised to make sure that security patches for legacy products will remain available. But even w/o such a promise it is OK because one can download and keep them by himself.

I don't jump on every new version MS releases. I do it only on "have to" basis either because of HW or SW applications requirements. I am fairly happy with W2K for development (and Office 2K). Others, such as WXP I use only for testing.

Originally the MSSecure.xml file used by 1.2.1 was to be discontinued 6 months after 2.0 released, but I believe they extended that (I do not recall until when)

Even for MBSA ver 2.0.1, I could not find the scan file, especially the new one.

You are correct that info on where to get the offline file is very, very thoroughly buried, and since v2 it has no longer been as simple as grabbing the file from disk on a system attached to the network after running mbsacli

The download link for the offline WsusScn2.cab file is mentioned in <http://support.microsoft.com/kb/926464>
For the more on the change from WsusScan.cab to the new format see <http://support.microsoft.com/kb/927745>

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