

Re: How to fix broken security in Windows 2000?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-02/0265.html>

From: Shannon Jacobs (*shanen_at_my-deja.com*)

Date: 02/07/05

Date: Mon, 7 Feb 2005 12:00:41 +0900

Where? If you are referring to <http://support.microsoft.com/default.aspx/kb/822798> (the only link I can find in a sampling of your posts in this thread), then you are incorrect (again). I just reviewed it (again) and that Web page does NOT answer the question, and is only tangentially related to the problem (via a special case). Part of the final section would be relevant (though I already know this is not the most convenient way to do it) *IF* there was some way to explicitly identify the missing certificates using SFC or some other tool. Or are you referring to some other link?

However, over the course of the several months in which I've been pursuing this problem, I almost surely read, studied, and performed the distantly related steps from that linked page, along with MANY others. As I already reported, the only partial success I achieved was from non-Microsoft sources. It makes me wonder if perhaps the real reason Microsoft has so far avoided answering the question is because they no longer support Windows 2000 to that degree. Imaginary (but sadly plausible) Microsoftian dialog: "Oh! So you would like to know if you have valid operating system files? Shucks and darn it, but due to various obscure and secret technical considerations, it turns out Windows 2000 doesn't support that feature after SP2. Soooo sorry, but you'll just have to upgrade to Windows XP."

I also checked a few more machines with SFC, and so far my hypothesis that all W2K machines have the problem seems to be holding up (and I have not yet found the problem on any WXP machine). That means it would be fundamentally impossible to know whether or not a W2K machine has valid system files, unless you use the CD to restore the original system files. Of course that cure would be worse than the disease, since you would almost surely be *undoing* various security patches. Note that if all W2K machines are missing certain security certificates, then the frequently appearing suggestion (in many of Microsoft's "support" Web pages) of copying them (via export) from another W2K machine is not going to work, either.

By the way, I removed the general WindowsUpdate from the follow-ups since I think the intersection is too small there. At this point I do not believe it is really a general WindowsUpdate problem, though it quite probably results from the normal use of the W2K WindowsUpdate.

[One minor comment: Mr. Dilley's post contained far more problems than two words with typos. However, it is only a trivial courtesy to use a spelling checker. My comment was about the rudeness, not the bad spelling per se, but Mr. Dilley's rudeness was rather amusing (or even hypocritical) in a post that apparently accused someone else of rudeness. (Hard to be sure what his intended points were, since they were so badly expressed.)]

Karl Levinson, mvp wrote:

> "Shannon Jacobs" <shanen@my-deja.com> wrote in message
> news:eIyF5S%23CFHA.2756@TK2MSFTNGP12.phx.gbl...
>
>> from there. Many years ago the newsgroups had a positive SNR, but
>> nowadays zero-signal-and-downhill is the safe prediction.
>>
>> Just in case some technically competent person would be so kind as to
>> provide a useful answer, the technical question is:
>>
>> How can missing security certificates be identified (and "safely"
>> replaced)?
>
> As I said, the first link I posted, which you complained about, tells
> you EXACTLY how to do that. If the instructions in that link didn't
> work for you, please tell us what the results are, e.g. you tried
> everything on that list, and X happened or didn't happen. If you had
> tried everything on that list, you would now be able to tell us that
> your computer has all the relevant certificates, and we would then
> know that the problem has nothing to do with restoring deleted
> certificates as you still seem to believe. We could also rule out a
> number of other dependencies on file checking besides certificates,
> and move towards the real cause and solution.
>
> I thought you said in a previous post that you had fixed the problem,
> and pointed to a page that suggested you might have re-installed some
> MS patch or another.
>
>> experiences, I do believe I could escalate the issue, pay Microsoft
>> some "support" money, and someone at Microsoft would reveal the
>> answer, perhaps
>
> Phone support for problems caused by MS patches [which you blamed at
> times] is absolutely free. What more could you possibly want? Which
> other vendors do this for you? You might be charged if the problem
> was not due to a MS patch.
>
>> with a clause requiring me not to republish it in public places like
>> the newsgroups. After all, security almost entirely depends on
>> obscurity, as all good Microsoftians "know".
>
> Paranoia and FUD. The MS KB is the same one the paid MS support
> technicians use.
>

microsoft.public.security: Re: How to fix broken security in Windows 2000?

> *[I trimmed the rest of the huge post below as a courtesy to other*
> *readers here.]*