

Re: microsoft acknowledges problems with update

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-08/2619.html>

From: Jeff (*jeff_at_falsepart.com*)

Date: 08/02/04

Date: Mon, 2 Aug 2004 19:56:13 -0400

- > *The critical updates may have addressed a pre-existing vulnerability on*
- > *your system, Jeff. IOW you didn't have any problems until the update(s)*
- > *blocked the malware from functioning.*
- >
- > *Post your HT log to one of the recommended forums.*

Interesting thought.....

I saved the log. Which forum would be best?

BTW, I know a fair amount about viruses and spyware. Is hijackware not just another type of virus that should be picked up by an uptodate virus checker or am I missing something?

Thanks again

--

Jeff McPherson

Email address deliberately false to avoid spam

jeff@falsepart.com

Outgoing mail is certified Virus Free by AVG

"PA Bear" <PABear@mvps.org> wrote in message

news:eVAAhYOeEHA.3792@TK2MSFTNGP09.phx.gbl...

- > The critical updates may have addressed a pre-existing vulnerability on
- > your system, Jeff. IOW you didn't have any problems until the update(s)
- > blocked the malware from functioning.

>

- > Post your HT log to one of the recommended forums.

> --

> ~PA Bear

>

> Jeff wrote:

- > > I've used both Ad-aware and Spybot regularly for years, with regular
- > > updates, including of course after the disaster. They found nothing. I
- > > also have uptodate anti-virus software and the Zone Alarm firewall. All
- > > regularly and conscientiously updated.

>

- > > I am not familiar with CWS shredder but will add it to my armamentarium,
- > > though of course my system is now fixed.

>

- > > You are correct though, it was right after the July 13 updates that my

microsoft.public.windowsxp.general: Re: microsoft acknowledges problems with update

> > problems started. Because the July 13 critical updates included a
> > "cumulative IE update", I assumed it was the same cumulative IE update.
> > Sorry for the confusion.
> >
> > I will look into all the sites you suggested. I do have Hijack this, but
> > do not use it because it requires more knowledge than I have to not
> > delete good stuff too.
> >
> > Thanks for the help. I appreciate it. However my problems started
> > immediately after the critical upgrades.
> >
> >
> > "PA Bear" <PABear@mvps.org> wrote in message
> > news:e0HnqYMeEHA.3348@TK2MSFTNGP09.phx.gbl...
> >> The MS page to which you refer covers MS04-025 (AKA 867801), released
> >> 30
> >> Jul-04, not MS04-018 (AKA 823353).
> >>
> >> MS04-018 (823353) was released with several other updates on 13 Jul-04,
> >> any of which may have caused you problems:
> >> <http://www.microsoft.com/technet/security/bulletin/ms04-jul.msp>
> >>
> >> However, I suspect "hijackware" is the cause of your IE problems, Jeff.
> >> Check your system for "hijackware":
> >>
> >> Help with Hijackware
> >> <http://aumha.org/a/parasite.htm>
> >> <http://aumha.org/a/quickfix.htm>
> >> <http://mvps.org/winhelp2002/unwanted.htm>
> >> <http://inetexplorer.mvps.org/Darnit.htm>
> >>
> >> CoolWebSearch Chronicles
> >> <http://www.spywareinfo.com/~merijn/cwschronicles.html>
> >>
> >> Run these tools in the following order with nothing else running in
> >> background:
> >>
> >> 1. CWSshredder (fix all found)
> >>
> >> 2. Ad-Aware (fix all found)
> >>
> >> 3. Spybot (RTFM but generally fix everything in red)
> >>
> >> Important: You *must* seek updates for Ad-Aware, Spybot, etc., before
> >> each and every use, even "right out of the box". But even they can't
> >> catch everything, 24/7. When all else fails, HijackThis
> >> (<http://www.spywareinfo.com/~merijn/files/HijackThis.exe>) is the
> >> preferred tool to use. It will help you to both identify and remove
> >> any
> >> hijackware/spyware. **Post your files to
<http://forums.spywareinfo.com/>
> >> or <http://forum.aumha.org/viewforum.php?f=30> for expert analysis, not
> >> here.**
> >>
> >> [Alternate download pages for many of the above tools may be found at
> >> <http://aumha.org/a/parasite.htm>.]
> >>
> >> Also:
> >>
> >> 1. Download and run Stinger (<http://vil.nai.com/vil/stinger/>); then...
> >>
> >> 2. Update your virus definitions, enable Show Hidden Files

microsoft.public.windowsxp.general: Re: microsoft acknowledges problems with update

> >>
> >
> > (<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>)
> >> and then run a full system scan in Safe Mode
> >>
> >
> > (<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406>)
> >> with nothing else running in background. Note the files identified and
> >> removed then find the corresponding page for the file at your AV
maker's
> >> online support pages (e.g.,
> >>
> >
> >> (<http://securityresponse.symantec.com/avcenter/venc/data/adware.winfavorites.html>)
> >> and follow all Removal steps.
> >>
> >> WinXP Only (WinME similar): If this scan finds anything, create a new
> >> Restore Point then Disk Cleanup > More options > Delete all but the
most
> >> recent Restore Point.
> >>
> >> 3. Check in at Windows Update.
> >>
> >> So How Did I Get Infected Anyway?
> >> <http://boards.cexx.org/viewtopic.php?t=957>
> >> --
> >> HTH - Please Reply to This Thread
> >>
> >> ~Robear Dyer (PA Bear)
> >> MS MVP-Windows (IE/OE), AH-VSOP
> >>
> >> AumHa Forums
> >> <http://forum.aumha.org>
> >>
> >> What You Should Know About Spyware
> >> <http://www.microsoft.com/mscorp/twc/privacy/spyware.mspx>
> >>
> >> Jeff wrote:
> >>> Finally!
> >>>
> >>> Ever since I downloaded the Windows XP critical update "Cumulative
> >>> Security Update for Outlook Express 6 SP1 (KB823353)", my IE6 has been
> >>> unable to find URLs and the whole system crashes intermittently. I
was
> >>> only able to reuse the PC and IE6 to view websites after I restored
the
> >>> entire system partition from a backup done before that update. I
asked
> >>> for advice from the Windows XP, the IE6 newsls and although some
other
> >>> users wrote about similar problems, I mainly got answers from the
> >>> experts that the patch installed fine and everything should be just
> >>> fine and I should check for viruses, etc.. Finally, when viewing the
> >>> "Read more" for this update on the MS update screen, I now see
> >>> that MS acknowledges the problem and the version you now find when you
> >>> click on the Windows update is apparently a new one dated August 1.
> >>> (You only find this by reading the hidden details in the "Read more"
> >>> section).
> >>>
> >>> Here is what MS writes:
> >>>
> >>> "Caveats: Subsequent to the release of this security bulletin,

microsoft.public.windowsxp.general: Re: microsoft acknowledges problems with update

Microsoft

```
> >>> was made aware that the update provided for Windows XP customers
running
> >>> the new version of Windows Update, Windows Update Version 5, did not
> >>> contain the final release code for the vulnerabilities addressed in
the
> >>> security bulletin. Microsoft has corrected the update and is
> >>> re-releasing this bulletin to advise of the availability of a revised
> >>> update available to Windows Update Version 5 customers. Customers who
> >>> are utilizing Windows Update Version 4, the vast majority of
customers,
> >>> are not affected by this revision."
> >>>
> >>> I have to admit I have yet to have the courage to install this revised
> >>> critical update <grin>. I'll make sure I have full partition backups
> >>> before I do it again. Using my Windows XP restore function was not
> >>> successful in removing the damage from that update.
>
```