

RE: MSBLASTER Infecting despite 03-026 patch?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-08/0199.html>

From: Joe Blatz (*sd_wireless_at_yahoo.com*)

Date: 08/14/03

Date: Thu, 14 Aug 2003 08:08:38 -0700 (PDT)

To: Jonathan Bloomquist <bocasolutions@yahoo.com>, incidents@securityfocus.com

No. No! NO!

Do not use the presence of the registry key. This is no more effective than WindowsUpdate or UpdateExpert.

Check for the files listed here:

<http://support.microsoft.com/?kbid=823980>

That is how to tell whether or not the patch is fully installed.

--- Jonathan Bloomquist <bocasolutions@yahoo.com> wrote:

> *I have been using the Retina DCOM scanner and it is*
> *working very well. After patching some systems,*
> *they*
> *still scanned as vulnerable. On NT, we were using*
> *the*
> *presence of the registry key*
> *HKLM\Software\Microsoft\Windows NT\Current*
> *Version\Hotfix\Q823980 to verify that the*
> *workstations*
> *were patched, but I found a workstation that had the*
> *registry key, but still scanned as vulnerable.*
>
> *Apparently something interfered with the*
> *installation*
> *before the .dlls or .exe could be loaded but after*
> *the*
> *registry key was created. Repatching the affected*
> *systems fixed them.*
>
> *This seemed to happen on workstations that were not*
> *up*
> *to service pack 6a. The hotfix would terminate and*
> *the user would reboot without noticing the error.*
>
> --- Marc Maiffret <marc@eeye.com> wrote:

SecurityFocus Incidents: RE: MSBLASTER Infecting despite 03-026 patch?

> > *I cant speak for the other tools but Retina's*
> *latest*
> > *version of the check*
> > *should be rather accurate. If your having any*
> > *problems though let me know.*
> >
> > *Signed,*
> > *Marc Maiffret*
> > *Chief Hacking Officer*
> > *eEye Digital Security*
> > *T.949.349.9062*
> > *F.949.349.9538*
> > *<http://eEye.com/Retina> – Network Security Scanner*
> > *<http://eEye.com/Iris> – Network Traffic Analyzer*
> > *<http://eEye.com/SecureIIS> – Stop known and unknown*
> > *IIS vulnerabilities*
> >
> > | -----Original Message-----
> > | *From: Carter, Mike*
> > | *[mailto:Mike_Carter@jdedwards.com]*
> > | *Sent: Monday, August 11, 2003 10:35 PM*
> > | *To: Charles Hamby; incidents@securityfocus.com*
> > | *Subject: RE: MSBLASTER Infecting despite 03-026*
> > *patch?*
> > |
> > |
> > | *This is something that really worries me, I've*
> > *heard it to.*
> > | *Also I am getting conflicting results when*
> > *scanning for the patch*
> > | *installation. I've been using MBSA, GFI LANguard*
> > *and Retina which all*
> > | *tell me something different.*
> > | *Which one should I trust??*
> > | *Or is there something else I should be using?*
> > |
> > | *Thanks*
> > | *Mike*
> > |
> > | -----Original Message-----
> > | *From: Charles Hamby [mailto:fixer@gci.net]*
> > | *Sent: Tuesday, August 12, 2003 5:13 PM*
> > | *To: incidents@securityfocus.com*
> > | *Subject: MSBLASTER Infecting despite 03-026*
> *patch?*
> > |
> > |
> > | *I have seen, and have heard other reports of,*
> > *msblaster.exe worm*
> > | *infecting a Windows computer that had the proper*
> > *KB patch specified by*

RE: MSBLASTER Infecting despite 03-026 patch?

SecurityFocus Incidents: RE: MSBLASTER Infecting despite 03-026 patch?

> > | *the 03-026 advisory. In the instance I*
> *personally*
> > *saw it was a Windows*
> > | *XP Professional workstation that was completely*
> > *patched. The person who*
> > | *used the workstation was surprised that they*
> *were*
> > *infected since they*
> > | *has applied the patch and I verified (via*
> > *Add/Remove Programs) that they*
> > | *did, indeed have the proper patch applied. I*
> > *checked with my parent*
> > | *organization and they had been receiving*
> *sporadic*
> > *reports of patched*
> > | *machines being infected despite being patched.*
> > *Unfortunately I removed*
> > | *the worm from the computer without copying it so*
> *I*
> > *don't have a backup*
> > | *of it for analysis.*
> > |
> > |
> > |
> > | *Has anyone else been seeing this phenomenon or*
> *do*
> > *they have any idea why*
> > | *this might have or might be happening? I know*
> *for*
> > *a fact the patch that*
> > | *was used came straight from Microsoft so I don't*
> > *suspect a faulty patch.*
> > |
> > |
> > | *Charles Hamby*
> > |
> > |
> > |
> >
>

> > | ----
> > |
> >
>

> > | ----
> > |
> > |
> > |
> >

SecurityFocus Incidents: RE: MSBLASTER Infecting despite 03-026 patch?

>

>> / -----

>> /

>>

>

>> / -----

>> /

>> /

>>

>>

>>

>

>>

>

>>

>>

>>

>

>

> =====

> *Jonathan Bloomquist, CISSP*

>

>

> *Do you Yahoo!?*

> *Yahoo! SiteBuilder – Free, easy-to-use web site*

> *design software*

> <http://sitebuilder.yahoo.com>

>

>

>

>

Do you Yahoo!?

Yahoo! SiteBuilder – Free, easy-to-use web site design software

<http://sitebuilder.yahoo.com>
