

Re: Microsoft Security Bulletin MS03-007 – 815021

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-03/1594.html>

From: Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP] (sbradcpa@pacbell.net)

Date: 03/18/03

Date: Mon, 17 Mar 2003 17:58:39 -0800

From: "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@pacbell.net>

Re: Alert: Microsoft Security Bulletin – MS03-007

Date:

Mon, 17 Mar 2003 14:20:30 -0700

From:

"M. Burnett" <mb@XATO.NET>

Reply-To:

Windows NTBugtraq Mailing List <NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM>

To:

NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Just to clarify, Microsoft's bulletin states that this vulnerability could have been prevented using URLScan and/or IISLockdown, but it isn't really specific on how to do this. Several people have asked me how this can be done.

The following steps can be used to block the attack:

1. Completely disable WebDAV by setting the HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\DisableWebDAV registry key to 1
2. Limit the length of requests (the url and any headers) by setting the HKLM\SYSTEM\CurrentControlSet\Services\w3svc\parameters MaxClientRequestBuffer to something like 16k
3. Block the following WebDAV HTTP verbs using URLScan (either by specifically blocking them or by not listing them as allowed):
OPTIONS, PROPFIND, PROPPATCH, MKCOL, DELETE, PUT, COPY, MOVE, LOCK, UNLOCK, OPTIONS, and SEARCH. Note that FrontPage does require the OPTIONS method to work properly.
4. Block the following WebDAV-related headers using the [DenyHeaders] section of URLScan.ini:
[DenyHeaders]
DAV:
Depth:

Destination:
If:
Label:
Lock-Token:
Overwrite:
TimeOut:
TimeType:
DAVTimeOutVal:
Other:

5. If you require WebDAV, you can limit the length of each individual header with these entries in the [RequestLimits] section (The exact values are obviously pretty generic and may need to be increased or decreased based on your particular configuration):

[RequestLimits]
Max-DAV=250
Max-Depth=250
Max-Destination=250
Max-If=250
Max-Label=250
Max-Lock-Token=250
Max-Overwrite=250
Max-TimeOut=250
Max-TimeType=250
Max-DAVTimeOutVal=250
Max-Other=250

Microsoft does not specifically state which HTTP Verb and/or header is affected, but it does say that it is related to WebDAV. I would therefore assume that setting ACLs on httpext.dll would still be effective in blocking the attack. The PUT and DELETE methods are still available in IIS, but only as part of the original HTTP spec, not part of WebDAV.

Mark Burnett
www.iisecurity.info

> *Microsoft have produced a pretty comprehensive web page discussing this*
> *vulnerability and the many things you should (could) do to prevent*
> *future attacks. Well worth the read;*
>
> <http://support.microsoft.com/default.aspx?scid=kb;en-us:816930>

Gordon Price wrote:

> "Dane" <Dane352@hotmail.com> wrote in message
> news:OfRwuSN7CHA.2328@TK2MSFTNGP10.phx.gbl...
>> *CERT's warning about the flaw is sober. "Any attacker who can reach a*
>> *vulnerable Web server can gain complete control of the system," it says.*

> > *"Note that this may be significantly more serious than a simple 'Web
> > defacement.' "*

>

> *On the flip side, how much testing has MS done? Are we going to find out
> that 10% of people who install the 'fix' are protected from the hack,
> because there server crashed and wouldn't come back. This is a little worse
> than a 'defacement' also. I am surprised that MS doesn't just fix IIS the
> way they did Outlook, you know, if anyone actually tries to connect to IIS
> you get an event that says "Potentially unsafe access blocked" and IIS just
> sits there, doing nothing. If this is MSs idea of Secure Computing I think
> someone must be smoking crack!*

>

> *Gordon*