

FW: Microsoft Security Advisory MS 03-007

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-03/0084.html>

From: Nero, Nick (Nick.Nero@disney.com)

Date: 03/18/03

Date: Tue, 18 Mar 2003 13:35:25 -0500
From: "Nero, Nick" <Nick.Nero@disney.com>
To: "Focus-MS" <focus-ms@securityfocus.com>

From: Nero, Nick

Sent: Tuesday, March 18, 2003 1:29 PM

To: 'Jonathan Grotegut'; Matthew Cole; Douglas R. Wilson; Focus-MS

I read at the XForce site, I believe, that Win2k3 RC2 (IIS6) is fine. I am trying to find a vulnerability tester/script and I could test it out myself. Anybody seen one?

From: Jonathan Grotegut [<mailto:jgrotegut@directpointe.com>]

Sent: Tuesday, March 18, 2003 12:27 PM

To: Matthew Cole; Douglas R. Wilson; Focus-MS

Matthew,

My understanding is this only affects the ntdll.dll file on Windows 2000 machines running IIS 5

Jonathan Grotegut

DirectPointe

-----Original Message-----

From: Matthew Cole [<mailto:mcole@sigpc.com>]

Sent: Tuesday, March 18, 2003 10:08 AM

To: Douglas R. Wilson; Focus-MS

Subject: RE: Microsoft Security Advisory MS 03-007

One of the websites I was reading (I think it was MS) referenced a Department of the Army server that had been compromised and that this patch was the result of the investigation into how this was done.

Has anyone heard if the Win 2003 RC2 Beta is vulnerable? The announcement covers IIS 5.1 but not IIS 6, and MS has not been particularly responsive patching beta code.

-----Original Message-----

From: Douglas R. Wilson [<mailto:dallendoug@dallenhome.org>]

FW: Microsoft Security Advisory MS 03-007

SecurityFocus Microsoft: FW: Microsoft Security Advisory MS 03-007

Sent: Monday, March 17, 2003 10:17 PM
To: Focus-MS
Subject: Re: Microsoft Security Advisory MS 03-007

some additional notes from emails I have recieved ---

> Douglas,
> You say "IIS servers are actively being compromised already, before
> the bulletin was released" --- do you have any links to documentation
> about this? I haven't heard of this.
>
> Also, besides IIS, what methods are available to exploit the
> vulnerability in ntdll.dll ?"

I must admit, I don't want to be scaremongerish. One published article that is low on details is at

<http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=22029>

"It is possible for remote attackers to run arbitrary code on vulnerable Web servers. This vulnerability is currently being exploited in the wild, and X-Force has verified the existence of a functional exploit tool. This vulnerability is in itself very serious, but the existence of robust exploits in the wild dictates that fixes or temporary workarounds should be applied immediately."

I also have some internal/proprietary information that I can't discuss that makes me believe similar. I will also admit that I have not seen firsthand evidence of a working compromise yet.

> On Mon, 2003-03-17 at 16:02, Douglas R. Wilson wrote:
> > The following test can be used:
> >
> >
> > If the C:\winnt\system32\inetsrv\httpext.dll file has ACL's on it
> > such that anonymous web context accounts cannot execute it, the
> > server in question is very likely not vulnerable to this exploit.
> > (Obviously, if you start considering the concept of NT
> > Authentication, and various user accounts accessing the httpext.dll,
> > the scope varies).
>
> But the MS advisory warns of SYSTEM access if compromised. Doesn't that
> mean that whatever crashes happens before IIS switches user context?

What I meant was as follows ---

the normal path of the exploit would be (very approximated --- I'm guessing

here)

- Anonymous request to webdav provider (httpext.dll)
- permissions are checked on httpext.dll to see if Anonymous request using Anonymous context can be processed
- internal request from httpext.dll to ntdll.dll (somewhere in the processing)
- ntdll.dll has buffer overflow condition

On a server that has been "locked down," because the anonymous request doesn't have permission to execute a call to the httpext.dll, the process is stopped.

However, if you are using basic and/or NT authentication, the web request is in the context of the user. so, the process would then be:

- User request to webdav provider (httpext.dll)
- permissions are checked on httpext.dll to see if User request using User context can be processed
- internal request from httpext.dll to ntdll.dll (somewhere in the processing)
- ntdll.dll has buffer overflow condition

Please note that in the second instance, the second step doesn't stop the process if anonymous user permissions are removed. The request would go through, and if it carried the exploit, compromise could occur. I wasn't envisioning a switch in context -- the person would be doing the exploit in the context of the user directly in the exception I envisioned. (i.e., a user logs into a website, and then, while logged in, feeds the overflow (or, more likely, a compromised account is used to do this to get around the lockout on anonymous))

I appreciate the comments so far! keep them coming!

Thanks,

Doug

--
Douglas R. Wilson
dallendoug@dallenhome.org

--
"the biologist will tell you that progress is the result of mutations. mutations are another word for freaks. for god's sake let's have a little more freakish behavior- not less . . . Maybe 90 per cent of the freaks will just be freaks, ludicrous and pathetic and getting nowhere but into trouble. . . Eliminate them, however- bully them into conformity- and nobody in america will ever be really young any more and we'll be left standing in the dead center of nowhere."
-- Tennessee Williams
----- Original Message -----

SecurityFocus Microsoft: FW: Microsoft Security Advisory MS 03-007

From: "Douglas R. Wilson" <dallendoug@dallenhome.org>

To: "Focus-MS" <focus-ms@securityfocus.com>

Sent: Monday, March 17, 2003 5:02 PM

Subject: Microsoft Security Advisory MS 03-007

I developed this for my work environment -- however, I believe that it isn't proprietary, and am forwarding it to the list for comment and/or informative values. Hopefully there are no glaring errors.

Please realize that any information contained in here should be verified and tested independently before you apply the process to any environment you are responsible for. I take no responsibility for any modifications anyone makes to their system based on what I put down here.

--

I have done some research today, as many people have asked the "are my web servers vulnerable/need to be patched, et al" question in response to the latest MSFT advisory (MS 03-007). It's likely that most servers that can be patched should be, BUT only after testing, as this may be a much more impactful problem than first realized, as well as all the other innate problems inherent with rolling patches out on production systems.

Microsoft has handled this somewhat differently than a standard bulletin, and the conjecture on that could easily be a separate discussion. Initially, however, it points to the fact that this vulnerability is with ALL Windows 2000 servers, period, and they have come out with this patch at this time because IIS servers are actively being compromised already, before the bulletin was released, to deal with an active attack vector. This implies that they may have rushed the patch out the door, and that the problems may involve a lot more parts of windows . . .

Points to consider:

* This may not be something that is an immediate threat to a lot of the servers if you only consider the IIS attack vector, if they have been deployed with the IIS lockdown tool in most configurations. CERTAIN CONFIGURATIONS OF THE IIS LOCKDOWN TOOL DO LEAVE WEBDAV ENABLED -- other methods should be employed there. There is a list of these profiles that I have found at the end of this.

* The servers in question may have other things impacted by the patch, as a core system dll is what is being replaced by this hotfix.

* The servers in question may not be able to be rebooted right away in keeping with SLA's/production schedules.

This is an issue with a core dll, ntdll.dll, which (I believe) is currently being addressed because an exploit exists that can be injected using IIS as its attack vector. MSFT recommends the IIS lockdown tool as one specific solution. However, some people are not sure they have applied the tool properly, and some people have made modifications and/or installed other applications since then (like Cold Fusion) that may add/modify application mappings, and thus change settings done by the IISLockdown tool.

I have derived one result from my research as a way to detect one form of "protection" from the exploit. This only addresses nailing down the IIS based attack vector, and only on certain boxes. However, the only true way to know for sure is if you have the exploit tool, and try using it, and it fails.

WebDAV requests are processed in the httpext.dll. This is NOT the dll that the buffer overflow exists in, but it is the dll that initially would handle WebDAV requests, and it is that dll which the IISLockdown tool "locks down."

So, if a windows 2000 server is running IIS 5.0, and it has

SecurityFocus Microsoft: FW: Microsoft Security Advisory MS 03-007

had either:

- * Service Pack 3 for windows 2000 installed, or
- * Service Pack 2 and MS02-018: April 2002

Cumulative Patch for Internet Information Services installed, or later cumulative patches installed,

The following test can be used:

If the C:\winnt\system32\inet_srv\httpext.dll file has ACL's

on it such that anonymous web context accounts cannot execute it, the server in question is very likely not vulnerable to this exploit. (Obviously, if you start considering the concept of NT Authentication, and various user accounts accessing the httpext.dll, the scope varies).

Older versions of the lockdown tool will simply deny the Everyone Group's permissions to execute -? as long as the anonymous users haven't been put in any privileged group, this is fine. Newer versions of the lockdown tool will create specific groups for web users, and then specifically deny permissions on these files.

The reason the service pack level is important is before MS02-018, some WebDAV requests could get around the httpext.dll, due to another issue, which is patched in either MS02-018 or SP3.

There may be some way of scripting up a tool that will check for the above parameters on servers, to do quick spot checking, if someone has not already developed a vulnerability testing tool. As I said before, however, the only true way to make sure is to attempt the exploit, and have it fail.

IIS Lockdown 2.1 Profiles that leave WebDAV enabled:

Small Business Server 2000

Exchange 2000 (OWA, PF, IM, SMTP, NNTP)

Share Point Portal Server

BizTalk Server 2000

Commerce Server 2000

Initial public release as pertains to Windows 2000:

http://www.microsoft.com/security/security_bulletins/ms03-007.asp

The full bulletin, as pertains to IIS:

<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-007.asp>

Article on WebDAV getting around httpext.dll in earlier versions:

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B307934>

IIS Lockdown Tool 2.1

<http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iisloc>

sloc

kd.exe

--

Douglas R. Wilson

dallendoug@dallenhome.org

--

"the biologist will tell you that progress is the result of mutations. mutations are another word for freaks. for god's sake let's have a little more freakish behavior- not less . . . Maybe 90 per cent of the freaks will just be freaks, ludicrous and pathetic and getting nowhere but into trouble. . . Eliminate them, however- bully them into conformity- and nobody in america will ever be really young any more and we'll be left standing in the dead center of nowhere."

-- Tennessee Williams

ALERT: How a Hacker Uses SQL Injection to Steal Your SQL Data! It's as simple as placing additional SQL commands into a Web Form input box giving hackers complete access to all your backend systems!

<http://www.spidynamics.com/mktg/sqlinjection33>

SecurityFocus Microsoft: FW: Microsoft Security Advisory MS 03-007

ALERT: How a Hacker Uses SQL Injection to Steal Your SQL Data! It's as simple as placing additional SQL commands into a Web Form input box giving hackers complete access to all your backend systems!
<http://www.spidynamics.com/mktg/sqlinjection33>

ALERT: How a Hacker Uses SQL Injection to Steal Your SQL Data! It's as simple as placing additional SQL commands into a Web Form input box giving hackers complete access to all your backend systems!
<http://www.spidynamics.com/mktg/sqlinjection33>

ALERT: How a Hacker Uses SQL Injection to Steal Your SQL Data!
It's as simple as placing additional SQL commands into a Web Form input box giving hackers complete access to all your backend systems!
<http://www.spidynamics.com/mktg/sqlinjection33>

ALERT: How a Hacker Uses SQL Injection to Steal Your SQL Data!
It's as simple as placing additional SQL commands into a Web Form input box giving hackers complete access to all your backend systems!
<http://www.spidynamics.com/mktg/sqlinjection33>