

RE: Question: Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-11/0134.html>

From: Fraser Hugh (hugh_fraser@dofasco.ca)

Date: 11/28/02

From: Fraser Hugh <hugh_fraser@dofasco.ca>

To: "'Hayes, Bill'" <Bill.Hayes@owh.com>, "Harris, Ken" <KHarris@HIPUSA.com>, focus-ms@securityfocus.com

Date: Thu, 28 Nov 2002 15:04:59 -0500

Microsoft web site indicates that a backout isn't recommended... that a re-deploy is needed to undo the upgrade. Our experience is that 2.6 is a subset of 2.7, and downgrading from 2.7 to 2.6 appears to work correctly, but there are vestiges of 2.7 left behind (to be expected since it's a subset). It's not a re-assuring state to be in.

> -----Original Message-----

> From: Hayes, Bill [<mailto:Bill.Hayes@owh.com>]

> Sent: Wednesday, November 27, 2002 2:24 PM

> To: Harris, Ken; focus-ms@securityfocus.com

> Subject: RE: Question: Buffer Overrun in Microsoft Data Access

> Components Could Lead to Code Execution (Q329414)

>

>

> Before you upgrade to MDAC 2.7, check with your vendors, even ones you
> don't think would have a problem. You might be surprised.

>

> For instance, I've heard ClearSwift is not supporting MAILsweeper
> installations with MDAC 2.7. Does anyone know if this is true? Is it
> just a temporary situation?

>

> Out of curiosity, has anyone attempted back out of MDAC 2.7 and go to
> MDAC 2.6 with patch? How bad was it?

>

> Bill...

>

> -----Original Message-----

> From: Harris, Ken [<mailto:KHarris@HIPUSA.com>]

> Sent: Tuesday, November 26, 2002 2:16 PM

> To: 'Kolde, Jennifer E.'; focus-ms@securityfocus.com

> Subject: RE: Question: Buffer Overrun in Microsoft Data Access

> Components Could Lead to Code Execution (Q329414)

>

RE: Question: Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)

>
> *Hello,*
>
> *Thanks to all on focus-ms who replied, very good information*
> *indeed. It*
> *looks like the best practice is to upgrade across the board*
> *to MDAC 2.7*
> *(with proper testing) /unless/ there is a known inoperability*
> *requiring*
> *2.6,*
> *in which case the patch is our best (albeit weak) hope.*
>
> *Thanks again for your help,*
>
> *Ken Harris*
>
> -----Original Message-----
> *From: Kolde, Jennifer E. [mailto:jkolde@nosc.mil]*
> *Sent: Tuesday, November 26, 2002 1:21 PM*
> *To: Harris, Ken; 'focus-ms@securityfocus.com'*
> *Subject: RE: Question: Buffer Overrun in Microsoft Data Access*
> *Components*
> *Could Lead to Code Execution (Q329414)*
>
>
> *Hello Ken,*
>
> *Sorry, trying again minus the digital signature.*
>
> *Microsoft also (quietly) lists upgrading to MDAC 2.7 as*
> *another fix. The*
> *information in the security bulletin is a bit confusing when*
> *you try to*
> *figure out just what is going on and where the vulnerability lies. The*
> *way I*
> *read it, the problem lies both the version of MDAC used AND a specific*
> *ActiveX control that is vulnerable. You are correct that even if you*
> *patch*
> *your current version of MDAC, the vulnerable ActiveX control*
> *could still*
> *be*
> *introduced.*
>
> *MDAC 2.7 is not vulnerable to the problem according to*
> *Microsoft, so if*
> *you*
> *upgrade to 2.7, the ActiveX issue becomes moot.*
>
> *A possible concern is that, because MDAC brokers your*
> *database requests,*
> *the*

- > upgrade may affect your application based on any differences
- > between the
- > older MDAC components and 2.7. I'm not a database guru
- > (IANADBG???) so
- > you'd have to research/test this on your own.
- >
- > MDAC can be downloaded from <http://www.microsoft.com/data/>, which also
- > includes documentation / changelogs for different versions. I did
- > install
- > MDAC 2.7 on a Win2K Server with no ill effects, but the Server is not
- > doing
- > anything specifically database-related.
- >
- > Regards,
- > Jennifer
- >
- > -----Original Message-----
- > From: Harris, Ken [mailto:KHarris@HIPUSA.com]
- > Sent: Friday, November 22, 2002 2:39 PM
- > To: 'focus-ms@securityfocus.com'
- > Subject: Question: Buffer Overrun in Microsoft Data Access Components
- > Could
- > Lead to Code Execution (Q329414)
- >
- >
- > Hello all on focus-ms,
- >
- > Was wondering if anyone had figured out the best practice fix to the
- > security flaw described here:
- >
- > [http://www.microsoft.com/technet/treeview/default.asp?url=/tec](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/securety/bulletin/MS02-065.asp)
- > [hnet/secure](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/securety/bulletin/MS02-065.asp)
- > [ty/](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/securety/bulletin/MS02-065.asp)
- > [bulletin/MS02-065.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/securety/bulletin/MS02-065.asp)
- >
- > The reason I ask is that Microsoft does not seem to show much
- > confidence
- > in
- > this patch; e.g. in the Caveats section, it is implied that
- > if a webpage
- > references the older, pre-patch RDS control, dependent upon the IE
- > security
- > settings they will either be prompted to install the control,
- > or it will
- > be
- > installed silently if Microsoft is added to the Trusted
- > Publishers list.
- >
- >
- > We happen to have a mission-critical custom webapp used
- > internally which

> does use RDS, and is in the Trusted Sites zone on our workstations.
 > However,
 > I can't guarantee that the developers of this solution will get around
 > to
 > patching the server on which this runs, or changing the references in
 > the
 > ASP pages. Microsoft is NOT in the Trusted Publishers list on our
 > workstation build, although there is nothing keeping our users from
 > clicking
 > "Always trust content from Microsoft".
 >
 > Am I right in assuming that even if we deploy the patch to our
 > workstations,
 > unless the patch is also applied to the webapp and the code
 > is changed,
 > the
 > vulnerable control could be reinstalled and the workstation would be
 > again
 > vulnerable to this attack from a malicious website? Is there a better
 > option? The client/server nature of this vulnerability makes me think
 > that
 > we may see a worm written to exploit it soon.

>
 > Thanks in advance.
 >
 > Regards,
 >
 > Ken Harris

> *****

> This message is a PRIVILEGED AND CONFIDENTIAL communication, and is
 > intended
 > only for the individual(s) named herein or others specifically
 > authorized to
 > receive the communication. If you are not the intended recipient, you
 > are
 > hereby notified that any dissemination, distribution or
 > copying of this
 > communication is strictly prohibited. If you have received this
 > communication in error, please notify the sender of the error
 > immediately,
 > do not read or use the communication in any manner, destroy
 > all copies,
 > and
 > delete it from your system if the communication was sent via email.

> *****

SecurityFocus Microsoft: RE: Question: Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution

>