

Re: Windows Media Player Remote Code Execution (923689) – sfpcopy. – sfpcopy.ex_ (0/1)

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-07/msg00000.html>

- *From:* "Steve Antonio [MSFT]" <steveant@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 02 Jul 2007 17:09:09 -0400
-

Attached...again, just rename to .exe

On Fri, 29 Jun 2007 08:10:01 -0700, Jonathan S. <Jonathan S.@xxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Steve,
I am having this same problem and was wondering if I could get a copy of this utility.
Thank you,
Jonathan S.

"Steve Antonio [MSFT]" wrote:

Here ya go...just rename to .exe

Hope this helps.

Steve Antonio, CISSP
Microsoft Exchange Support

On Sun, 6 May 2007 11:16:26 -0400, "Tony S"
<tbtony@xxxxxxxxxxxxxxxx>
wrote:

Microsoft is telling me that a workaround for this issue would be to rename, delete or move the un-patched version of WMP6.4 binary (dxmasf.dll) to help secure your system. Also, they are saying that we can replace the un-patched version of WMP6.4 binary (dxmasf.dll) with the patched version.

Unfortunately I have tried doing these steps without luck due

to System File Protection (Windows File Protection). I mentioned this to them and they tell me that I should be able to use the SFPCOPY.EXE tool/utility to do the trick. They say that this utility is included with every Windows installation, however, it does not seem to exist on any of the Windows servers in our organization. I have told them this and they say that they do not know why it is not on my systems, nor where the tool can be downloaded.

Does anyone know where I can find this SFPCOPY.EXE utility??

Any help would be greatly appreciated.

"Tony S" <tbtony@xxxxxxxxxxxxxxxxxxxx> wrote in message news:O0gyqH2iHHA.872@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Here is Microsoft Security–PSS' response:

"We are actively testing a fix for the issue described below. We will indeed release a fix for this issue. The current plan is to release a new package for Windows Server on June 12th (Patch Tuesday). The update will be noted in the "Revisions" section of the Security Bulletin for MS06–078. On June 12th you will be able to apply the new install package for Windows Server 2003 to secure your systems."

Tony

"Steve Antonio [MSFT]"
<steveant@xxxxxxxxxxxxxxxxxxxxxxxx> wrote
in message
news:3gj133th7r2v148pjuk0ldaqlqmg1cntql@xxxxxxxxxxxx

Ahh, so it does. Interesting
and also, not very
comforting.

I'm no longer with the
Security team here, so it

would be better for
you to call and open a case
(no charge since it's bulletin
related).

Just be sure to indicate it's a
problem with MS06-078).

The folks in PSS-Security
would be able to investigate
this with the
Windows Media team and
find out if there is a problem
in the detection
logic for the update.

Thanks for the heads up on
this!

-Steve

On Thu, 26 Apr 2007
08:24:03 -0400, "Tony S"
<tbtony@xxxxxxxxxxxxxxxxxxx>
wrote:

Steve,

When I run
mplayer2.exe
from this
Windows
Server 2003
SP2 box, it
runs
the
OLD
version of
Windows
Media
Player. I am
not talking
about Vista.
Please
confirm this
on your end
before you
repond
again.

Thank you,

Tony

"Steve
Antonio
[MSFT]"

<steveant@xxxxxxxxxxxxxxxxxxxxxx>

wrote in
message

news:3gmv2392e3isel1uo1fgtlhmu66qevoekv@xxxxxxxxxx

Running
mplayer2.exe
will
launch
the
most
updated
version
of
WMP
that
you
have.
For
instance
on
my
Vista
machine,
I
run
wmplayer2.exe
and
it
launches
WMP11.
It
will
not
use
the
old
dlls,
therefore
there
is
no
need
to
update

them.

On
Wed,
25
Apr
2007
18:16:37
-0400,
"Tony
S"
<tbtony@xxxxxxxxxxxxxxxxxxx>
wrote:

Here
is
what
the
vendor
said:

"Windows
media
player
6.4
is
installed
by
default
in
every
windows
installation
and
cannot
be
removed.
Simply
running
mplayer2.exe
from
program
files\windows
media
player\
is
enough
to
run
the

vulnerable
application,
even
if
it
is
not
the
default
association
for
media
content
types.
This
is
an
accurate
audit
and
you
should
follow
up
with
Microsoft
support."

Any
further
help
would
be
greatly
appreciated.

Thank
you,

Tony

"Steve
Antonio
[MSFT]"
<steveant@xxxxxxxxxxxxxxxxxxxxxxxx>
wrote
in
message

That's
the
version
for
Windows
Media
Player
6.4.
Since
you
are
running
WM10,
then
the
only
file
you
need
to
worry
about
is
wmvcore.dll
and
it
should
be
at
least
10.0.0.3708.

The
reason
6.4.9.1133
doesn't
get
updated
or
won't
install
on
SP2
is
because
it
isn't
used
anymore

when
WM10
is
on
the
machine.

Seems
like
the
security
auditor
doesn't
have
all
their
facts
straight.

Steve
Antonio,
CISSP

This
posting
is
provided
"AS
IS"
with
no
warranties,
and
confers
no
rights.

Use
of
included
script
samples
are
subject
to
the
terms
specified
at

<http://www.microsoft.com/info/copyright.htm>

Note:

For

the
benefit
of
the
community-at-large,
all
responses
to
this
message
are
best
directed
to
the
newsgroup/thread
from
which
they
originated.

On
Mon,
23
Apr
2007
16:36:24
-0400,
"Tony
S"
<tbtony@xxxxxxxxxxxxxxxxxxxx>
wrote:

Hello!

We
recently
self-audited
our
servers
and
found
that
one
of
them
has
this
high-risk
vulnerability.

To
reference
the
vulnerability
description,

"Multiple
vulnerabilities
in
Windows
Media
Player
could
allow
remote
code
execution.
One
vulnerability
relates
to
ASX
file
processing.
WMVCORE.DLL
contains
an
exploitable
heap
buffer
overflow
in
its
handling
of
"REF
HREF"
URLs
within
ASX
files.
As
ASX
files
are
opened
automatically
through
Internet
Explorer,
an

attacker
could
use
this
to
gain
remote
execution
privileges
at
the
level
of
the
user
simply
from
the
user
visiting
a
malicious
web
page.
The
other
relates
to
processing
ASF
files."

See
also
<http://support.microsoft.com/kb/923689>

The
OS
of
the
server
in
question
is
Windows
Server
2003
Standard
SP2
v5.2.3790.
The

DXMASF.DLL
file
on
this
system
is
version
6.4.9.1125
and
it
is
running
MS
Windows
Media
Player
version
10.
The
server
has
all
updates/patches
installed
according
to
the
Windows
Updates
site.
Apparantly
the
security
audit
software
looks
to
the
version
of
the
DXMASF.DLL
file
and
if
it
is
not
version
6.4.9.1133,
it

complains
that
the
vulnerability
exists.

The
security
audit
vendor
is
telling
me
"It
appears
the
file
dxmasf.dll
does
not
get
updated
by
SP2
as
it
should.
The
file
is
unmodified
by
the
service
pack.
So
if
you
patched
beforehand,
you
are
still
protected.
But
if
you
did
not
patch
prior

to
installing
service
pack
2,
you
are
now
unable
to
install
the
patch.
I
recommend
contacting
Microsoft
about
this,
as
it
looks
like
they
will
need
to
release
another
update
to
fix
this."

Please
help
us
to
rid
the
server
of
this
vulnerability.

Thank
you
in
advance,

Tony

S,
MCP
Network
Manager

Hope
this
helps.

Steve
Antonio,
CISSP
Microsoft
Exchange
Support

Hope this helps.

Steve Antonio, CISSP
Microsoft Exchange
Support

Hope this helps.

Steve Antonio, CISSP
Microsoft Exchange Support

.