

# Re: Windows Media Player Remote Code Execution (923689)

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-04/msg00112.html>

---

- *From:* "Tony S" <[tbtony@xxxxxxxxxxxxxxxxxxxx](mailto:tbtony@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 25 Apr 2007 18:16:37 -0400
- 

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@xxxxxxxxxxxxxxxxxxxx](mailto:steveant@xxxxxxxxxxxxxxxxxxxx)> wrote in message [news:qd7q2315hjah8u4d9fa2lin32c9t461mrg@xxxxxxxxxxx](mailto:news:qd7q2315hjah8u4d9fa2lin32c9t461mrg@xxxxxxxxxxx)

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.

Re: Windows Media Player Remote Code Execution (923689)

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

Re: Windows Media Player Remote Code Execution (923689)