

MS Windows Media Player 9 Vulns (2)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-12/0240.html>

From: Arman Nayyeri (*arman-n_at_Phreaker.net*)

Date: 12/18/04

Date: 18 Dec 2004 07:43:55 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

Microsoft Windows Media Player 9 Vulns

=====
Title: Microsoft Windows Media Player 9 Vulns (2)

HappyName: MS-WMP9-2P-BY-R^AN

Date: Friday, April 17, 2004

Software: Microsoft Windows Media Player 9

Vendor: Microsoft Corporation

Patch: Fixed in Microsoft Windows Media Player 10

Author: Arman Nayyeri, arman-n[at]phreaker[daat]net, <http://www.4rman.com>

Severity: As little as heaven! (seriously: Moderate)

Description:

=====
I have been reported this vulns on "Monday, July 05, 2004 4:11 PM" to microsoft. They finally corrected these flaws in WMP 10. So I just wait some time for some people to install WMP 10, now it's showtime!

Windows Media Player Allows Writing To Audio Files: (WMP-AWTAF)

=====
The Windows Media Player allow the name of artist and song be changed by using windows media player control in Internet explorer, so it will allow an attacker to overwrite the artist and album and song name of a music file by finding a mp3 file (for example).

It is not so much important itself but become more important if we can cause IE to parse the mp3 file then we can easily inject script in my computer zone, there is some default music files that exists when windows get installed (ME and XP), so it will become more easier to exploit.

something like this:

```
WindowsMediaPlayer.currentMedia.setItemInfo("Artist", '&lt;script&gt;alert("Hello");</'+script>);
```

but actually I never found such vuln in IE which cause such severity!

SecurityFocus Bugtraq: MS Windows Media Player 9 Vulns (2)

Because I'm so busy, take a look at "I need some help!" section.

So I left it as an exercise for the attacker ;)

Windows Media Player ActiveX Object Expose Existence Of Files: (WMP-AXOEEOF)

There is a way to determine if a file exists and if it exists find it's size. I have used the getItemInfoByAtom() function with a magical number. the magical number is 19 which actually used to get the file size. But we can open any (music or non-music) files by WMP ActiveX and call this function on it. it will return 0 if the file does not exists (or is empty) and return the size if it exists.

Exploit:

=====

The exploits for WMP-AWTAF and WMP-AXOEEOF (read it a'zoe'e'of) can be found at:

<http://www.4rman.com/security.htm>

enjoy my website. And you may also enjoy hackin' my website too!

<http://www.4rman.com>

Exploit Tested On

=====

Windows Media Player 9.0

on

Microsoft Windows XP

Microsoft Windows XP SP1

Microsoft Windows XP SP2

Vendor Status

=====

Microsoft notified about 6 month ago.

The bug fixed in Windows Media Player 10.

Special Thanks

=====

Special thanks to my FAMILY

Do I discover more vulnerabilities?

=====

I'm so busy these days.

Read below.

I need some help! HELP!! HELP!! HELP!!

=====

I'm in the way of my research and I actually need some help about viruses.

let me tell you some about my research:

I'm working on a virus defense system which does not rely on Virus Signatures at all. I used some ways to defend viruses and trojan when they want to spread or damage the computer. It's almost 8 months which I started this research. I called it Instantaneous

SecurityFocus Bugtraq: MS Windows Media Player 9 Vulns (2)

Defense Technology (IDT). I'm working alone. First of all I want to know if there is anyone who is interested in supporting me and my research. And if there is someone who really have nice info in this subject and can help me in this way. The beta version of a sample program based on IDT will be released in the next 6 months. Also I'm ready to cooperate with any company which have a nice offer for working in this subject. In march I will need some virus/trojan samples. If anyone have virus samples or knows how to get samples contact me. I will continue my research until I get a nice offer.

Disclaimer:

=====

Arman Nayyeri is not responsible for the misuse of the information provided in this advisory. The opinions expressed are my own and not of any company. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this advisory. Any use of the information is at the user's own risk.

~~~~~

and sorry for my f\*%#in' poor english,

Arman Nayyeri

From

Persia (or Iran)

<http://www.4rman.com>