Subject: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Mon, 02 Jan 2006 21:25:20 GMT
View Forum Message <> Reply to Message

Last week a vulnerability was found in all versions of windows that allows people to execute arbitrary code using a buffer over-run in Windows Metafiles.

WMF files are images, so can be placed on any website or email and can be used to attack your system.

Please, everyone read: http://grc.com/sn/notes-020.htm
Use this to see if your system is vulnerable:
http://www.hexblog.com/2006/01/wmf_vulnerability_checker.htm l
Use this to 3rd party patch to secure it:
http://www.hexblog.com/security/files/wmffix_hexblog13.exe

More technical details can be found here: http://www.f-secure.com/weblog/

EDIT:

Due to over-use, the hexblog website has been suspeneded. New Download links hosted on GRC.com

The Checker: http://www.grc.com/miscfiles/wmf_checker_hexblog.exe
and The Patcher: http://www.grc.com/miscfiles/wmffix_hexblog14.exe

EDIT 2:

A revised list of vulnerable OS's. Bascially the two main ones are XP and Server 2003.
http://blog.ziffdavis.com/seltzer/archive/2006/01/03/39684.a spx

F-Secure RSS Feed:

Larry Seltzer from eWeek has been doing lots of additional testing against older versions of Windows and bad WMF files.He has just blogged his interesting findings:...in a practical sense, only Windows XP and Windows Server 2003 (in all their service pack levels) are vulnerable to the WMF flaw.
...all versions of Windows back to 3.0 have the vulnerability in GDI32.

Except for Windows XP and Windows Server 2003, no Windows versions, in their default configuration, have a default association for WMF files, and none of their Paint programs or any other standard programs installed with them can read WMF files...So the vulnerability is there on all platforms but it seems that only Windows XP and 2003 are easily exploitable. Unfortunately this still means that majority of Windows computers out there are vulnerable right now. And at least Windows 2000 becomes vulnerable if you're using many of the available third party image handling programs to open image files. On 03/01/06 At 07:29 AMhttp://www.f-secure.com/weblog/#00000764

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Aprime on Mon, 02 Jan 2006 21:40:02 GMT
View Forum Message <> Reply to Message

It seems that many servers are affected by this, yesterday for instance my antivirus blocked 5 attempts to infect my computer using this method.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Mon, 02 Jan 2006 21:47:23 GMT
View Forum Message <> Reply to Message

Yeah, there are a lot of people who are trying to use this method to infect computers.

Anything from a website to an email attachment to an MSN link can do it.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by idebo on Mon, 02 Jan 2006 21:54:37 GMT
View Forum Message <> Reply to Message

Thanks for the info.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by icedog90 on Mon, 02 Jan 2006 22:15:16 GMT
View Forum Message <> Reply to Message

Thanks, my system turned out to be vulnerable.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by csskiller on Tue, 03 Jan 2006 05:09:06 GMT
View Forum Message <> Reply to Message

Thanks, I would have never found out if you hadn't told me.

Just when Microsoft was beginning to win back my vote...

Things by Microsoft that I hate:

X-Box
Windows (to an extent)
Microsoft Flight Simulator
X-Box 360
Halo

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Lijitsu on Tue, 03 Jan 2006 06:11:52 GMT
View Forum Message <> Reply to Message

Ooh, nice discovery. I've had the setup at the restart part for the last hour, like an idiot.

Oh, and thank you.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by xptek on Tue, 03 Jan 2006 06:13:55 GMT
View Forum Message <> Reply to Message

And then FreeBSD was born..

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Goztow on Tue, 03 Jan 2006 07:24:04 GMT
View Forum Message <> Reply to Message

Tx for notifying! Winamp r0x0rs .

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by RTsa on Tue, 03 Jan 2006 13:15:00 GMT
View Forum Message <> Reply to Message

Yes, this was actually in the Finnish news yesterday...
I didn't think it was too serious but I did check that my computer is vulnerable to this thing.

I guess I'll install the hotfix, thanks for the links

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by The Mad Hatter on Tue, 03 Jan 2006 13:25:04 GMT
View Forum Message <> Reply to Message

Thank you.

So once Microsoft release a fix you should uninstall the patch?

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Xtrm2Matt on Tue, 03 Jan 2006 19:03:00 GMT
View Forum Message <> Reply to Message

I don't think you realise how easy it is to infect people with this.

My signature could hold the virus for all you know. Only a decent AV can tell.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Spice on Tue, 03 Jan 2006 20:10:29 GMT
View Forum Message <> Reply to Message

Thanks, I just applied the patch.

csskiller wrote on Tue, 03 January 2006 00:09

Just when Microsoft was beginning to win back my vote...

Things by Microsoft that I hate:

Halo

Actually, Microsoft didn't make Halo, Bungie developed the game, Microsoft only published it. The game still sucks though.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Lijitsu on Tue, 03 Jan 2006 20:23:02 GMT
View Forum Message <> Reply to Message

EXdeath7 wrote on Tue, 03 January 2006 15:10Thanks, I just applied the patch.

csskiller wrote on Tue, 03 January 2006 00:09

Just when Microsoft was beginning to win back my vote...

Things by Microsoft that I hate:

Halo

Actually, Microsoft didn't make Halo, Bungie developed the game, Microsoft only published it. The game still sucks though.
Thank you for standing up for the game, but why do you hate it? I want a real answer, too. I've been getting shit like: "PC 1S B3774R 7H3N X80X!11!!ONE!" Yes, the PC is better than the Xbox, but the Xbox is a console. You can't upgrade a console like you can a PC.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Spice on Tue, 03 Jan 2006 22:00:15 GMT
View Forum Message <> Reply to Message

That... my friend, is a story for another topic.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Tue, 03 Jan 2006 23:29:00 GMT
View Forum Message <> Reply to Message

The Mad Hatter wrote on Wed, 04 January 2006 02:25Thank you.

So once Microsoft release a fix you should uninstall the patch?

Correct. Once Microsoft fix this issue, then you will have no need for this patch. It is a temporary measure.

Edit: Here is an updated list of vulnerable systems. Looks like pepole on 98/2000 are more secure than we thought. The two most vulnerable OS's are XP and Server 2003

It can be hidden in an image, so any image could do it, including Xtrm2Matt's signature.

For the record: Halo kicks ass.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by cmatt42 on Wed, 04 Jan 2006 00:18:19 GMT
View Forum Message <> Reply to Message

Quote:Account for domain hexblog.com has been suspended

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by csskiller on Wed, 04 Jan 2006 00:42:46 GMT
View Forum Message <> Reply to Message

Here are the programs that were on the site.
The first one being the checker and the second one being the patch

And although Halo kicks ass I still don't like it

File Attachments
1) wmf_checker_hexblog.exe, downloaded 145 times
2) wmffix_hexblog13.exe, downloaded 136 times

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Wed, 04 Jan 2006 04:04:43 GMT
View Forum Message <> Reply to Message

Ilfak Guilfanov's "HexBlog" web site has been administratively suspended due to excessive use. (Yeah, no kidding!) My recent eMail to Ilfak bounced with an "unknown recipient" error. You may retrieve Ilfak's latest files from the GRC server using the following links:

From: http://grc.com/sn/notes-020.htm

Download links, hosted on GRC.com

http://www.grc.com/miscfiles/wmffix_hexblog14.exe
http://www.grc.com/miscfiles/wmf_checker_hexblog.exe

Thanks csskiller for uploading them here too.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Xtrm2Matt on Thu, 05 Jan 2006 10:57:16 GMT
View Forum Message <> Reply to Message

You really shouldn't go and download an exe you know nothing about.

Use built-in Windows features to immune yourself:
Start > run > regsvr32 /u shimgvw.dll

To re-enable the dll, just do:
Start > run > regsvr32 shimgvw.dll

....

A side-effect is that it will disable viewing of thumbnails in Windows image thingy-whatever-ma-jick. Just use another image viewing program to do such a thing.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by The Mad Hatter on Thu, 05 Jan 2006 18:35:29 GMT
View Forum Message <> Reply to Message

Thanks for the info.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Dave Mason on Thu, 05 Jan 2006 22:31:29 GMT
View Forum Message <> Reply to Message

http://www.microsoft.com/athome/security/update/bulletins/20 0601_WMF.mspx

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Fri, 06 Jan 2006 01:11:00 GMT
View Forum Message <> Reply to Message

http://grc.com/sn/notes-020.htm << Explains pretty much everything.

The guy who wrote this released his source code too. People have looked over it and said it's fine.

Besides, your taking a bigger risk not patching.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Fri, 06 Jan 2006 02:21:26 GMT
View Forum Message <> Reply to Message

Xtrm2Matt wrote on Thu, 05 January 2006 23:57You really shouldn't go and download an exe you know nothing about.

Use built-in Windows features to immune yourself:
Start > run > regsvr32 /u shimgvw.dll

To re-enable the dll, just do:
Start > run > regsvr32 shimgvw.dll

....

A side-effect is that it will disable viewing of thumbnails in Windows image thingy-whatever-ma-jick. Just use another image viewing program to do such a thing.

Thats not a full fix. It just makes it harder to trigger the vulnerability.

However, I believe MS have released their patch now. (It does exactly them same thing as the 3rd party one)

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by Dave Mason on Fri, 06 Jan 2006 02:29:13 GMT
View Forum Message <> Reply to Message

Hence my link.

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch

Posted by Renx on Fri, 06 Jan 2006 03:15:41 GMT
View Forum Message <> Reply to Message

MS already released a fix for it. I downloaded it today while updating XP before I even knew about the vulnerability

Subject: Re: Everyone Read - Windows WMF Vulnerability Patch
Posted by light on Fri, 06 Jan 2006 03:30:38 GMT
View Forum Message <> Reply to Message

Renx wrote on Fri, 06 January 2006 16:15MS already released a fix for it. I downloaded it today while updating XP before I even knew about the vulnerability

It's just a shame they took so long. This should have been patched by them much sooner.

I will be patching when I get home.