

WMF exploit - Quick Guide

Updated 1/5/2006 8:31 PM GMT

Microsoft have announced that they will release a patch for this vulnerability early (as opposed to waiting for patch Tuesday). This update will be available via Windows Update and as a separate download ([available here](#)). More [details here](#).

I've started receiving a number of queries from readers who are both concerned and confused about the recent Windows MetaFile WMF exploit. So many in fact that I think that there isn't enough information out there in the public domain about this vulnerability as yet and I've decided to create a quick guide to the WMF exploit.

What is the WMF exploit?

A vulnerability has been discovered in Windows that allows a specially crafted WMF (Windows MetaFile) image file to run code contained within the image file without the consent or prompt. This code can be designed to do any number of things, from install viruses and worms, install adware or even trash the Windows operating system.

How is the code run?

The code is run when the WMF image is displayed. This exploit rewrites all the rules previously written about viewing images not being dangerous - viewing one of these altered WMF files can be really bad for your PC.

How can I be affected?

There are a number of ways that you can be affected. You can view affected WMF files in the browser, in an email, or instant message. All you need to do to be infected is *view* an image that contains the exploit.

Even if you don't view an affected WMF file you can still become infected if you have a drive indexing program such as Google Desktop installed. This is because some of these programs run the code during the indexing of the file.

What versions of Windows are affected?

All main versions - Microsoft have confirmed that Windows 98, Windows 98 SE, Windows ME, Windows 2000, Windows XP (Home and Professional) and Windows 2003 are affected.

Further research seems to show that Windows 98, Windows 98 SE and Windows ME might be [harder to infect than later versions](#), although they still contain the exploit and may be targeted with greater ferocity soon.

<http://www.pcdoctor-guide.com/wordpress/?p=2068>

Feel free to distribute

What products are affected?

Here is the current list from [SecurityFocus](#):

XnView XnView Standard 1.80.3
XnView XnView Minimal 1.80.3
XnView XnView Complete 1.80.3
Microsoft Windows XP Tablet PC Edition SP2
Microsoft Windows XP Tablet PC Edition SP1
Microsoft Windows XP Tablet PC Edition
Microsoft Windows XP Professional x64 Edition
Microsoft Windows XP Professional SP2
Microsoft Windows XP Professional SP1
Microsoft Windows XP Professional
Microsoft Windows XP Media Center Edition SP2
Microsoft Windows XP Media Center Edition SP1
Microsoft Windows XP Media Center Edition
Microsoft Windows XP Home SP2
Microsoft Windows XP Home SP1
Microsoft Windows XP Home
Microsoft Windows Server 2003 Web Edition SP1
Microsoft Windows Server 2003 Web Edition
Microsoft Windows Server 2003 Standard x64 Edition
Microsoft Windows Server 2003 Standard Edition SP1
Microsoft Windows Server 2003 Standard Edition
Microsoft Windows Server 2003 Enterprise x64 Edition
Microsoft Windows Server 2003 Enterprise Edition 64-bit SP1
Microsoft Windows Server 2003 Enterprise Edition 64-bit
Microsoft Windows Server 2003 Enterprise Edition SP1
Microsoft Windows Server 2003 Enterprise Edition
Microsoft Windows Server 2003 Datacenter x64 Edition
Microsoft Windows Server 2003 Datacenter Edition 64-bit SP1
Microsoft Windows Server 2003 Datacenter Edition 64-bit
Microsoft Windows Server 2003 Datacenter Edition SP1
Microsoft Windows Server 2003 Datacenter Edition
Microsoft Windows ME
Microsoft Windows 98SE
Microsoft Windows 98
Microsoft Windows 2000 Server SP4
Microsoft Windows 2000 Server SP3
Microsoft Windows 2000 Server SP2
Microsoft Windows 2000 Server SP1
Microsoft Windows 2000 Server
+ Avaya DefinityOne Media Servers
+ Avaya IP600 Media Servers
+ Avaya S3400 Message Application Server

<http://www.pcdactor-guide.com/wordpress/?p=2068>

Feel free to distribute

+ Avaya S8100 Media Servers
Microsoft Windows 2000 Professional SP4
Microsoft Windows 2000 Professional SP3
Microsoft Windows 2000 Professional SP2
Microsoft Windows 2000 Professional SP1
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Datacenter Server SP4
Microsoft Windows 2000 Datacenter Server SP3
Microsoft Windows 2000 Datacenter Server SP2
Microsoft Windows 2000 Datacenter Server SP1
Microsoft Windows 2000 Datacenter Server
Microsoft Windows 2000 Advanced Server SP4
Microsoft Windows 2000 Advanced Server SP3
Microsoft Windows 2000 Advanced Server SP2
Microsoft Windows 2000 Advanced Server SP1
Microsoft Windows 2000 Advanced Server
IrfanView IrfanView 3.98
IrfanView IrfanView 3.97
IrfanView IrfanView 3.95
IBM Lotus Notes 6.5.4
IBM Lotus Notes 6.5.3
IBM Lotus Notes 6.5.2
IBM Lotus Notes 6.5.1
IBM Lotus Notes 6.5

What if I switch from Internet Explorer to a different browser?

Makes no difference - It's not a browser vulnerability but a Windows issue.

Is this issue widespread?

Yes, very much so. Security experts have been tracking this exploit of the past few days and not only is it spreading fast but many new exploits are released daily.

If the vulnerability is confined to WMF files, can't I just block them?

No. What makes this issue much worse is the fact that the affected WMF files can be renamed as .JPG, .GIF, .BMP or a number of other different file extensions and the exploit code will still run. This is because Windows handles these files based on the header information contained in the image rather than based on the file extension.

Has Microsoft released a patch yet?

No. Microsoft are working on a patch and plan to make it available on during [January's Patch Tuesday \(January 10th\)](#).

<http://www.pedoctor-guide.com/wordpress/?p=2068>

Feel free to distribute

What can I do to protect myself?

There are a number of steps you can take to protect yourself.

1. First, make sure that you update your antivirus and antispyware applications on a daily basis (or twice daily for added security). Most vendors are releasing updates for exploits as they are being discovered and this provides the first line of defense.
2. Don't visit untrusted sites. You are far more likely to be infected on a site that makes illegal MP3s available for download than you are say on CNN.
3. You can unregister the DLL file that causes the code to be run in WMF when they are viewed automatically.
 - Click on **Start > Run**.
 - Type:
regsvr32 /u shimvw.dll
 - Click **OK**
 - Click **OK** again when the dialog appears.
4. Download and install the [Sunbelt Kerio Firewall \(free or full version\)](#) and install the Bleeding-Edge Snort rules (from [here](#)). There is more information on this from [Sunbelt](#).
5. Check to see if your PC supports hardware-enforced DEP (Data Execution Prevention). If it does then this provides some protection from the exploit. Right-click on **My Computer** and choose **Properties** followed by **Advanced**. Then, in the **Performance** section choose **Settings**. Now click on the tab labeled **Data Execution Prevention**. If your system is only protected by software-enforced DEP then you will see a message on the dialog box that says:

Your computer's processor does not support hardware-based DEP. However, Windows can use DEP software to help prevent some types of attacks.

To gain greater protection set hardware-enabled DEP to “all programs and services”.

6. There is also an unofficial patch, by Ilfak Guilfanov (the lead programmer responsible for IDA Pro, a tool used by security companies around the world). This patch (available [here](#)) removes the vulnerability in Windows but do bear in mind that this is an unofficial patch and might break other things (nothing has been reported as of yet though). Until Microsoft releases a patch this is the best way to remove the vulnerability.

IT IS NOW HIGHLY RECOMMENDED THAT YOU INSTALL THIS PATCH.

The updated version of this patch now works for Windows 2000 (SP4), Windows XP Home and Pro (32-bit and 64-bit) and Windows Server 2003.

You can download the SANS reverse engineered, reviewed, and vetted version from [here](#).

It seems that Ilfak Guilfanov Hexblog site has gone down (too much traffic) and he's in the process of moving. However, this means that people can't download the patches. I'll mirror them in the interim.

- [Hotfix version 1.4](#)
 - [WMF vulnerability checker](#)
7. There's another unofficial WMF patch available, this time from [Paolo Monti of Eset](#). The main difference between this patch and the patch by Ilfak Guilfanov is that this patch works on Windows 98/ME.

Can I check to see if I'm protected?

Yes. [Ilfak Guilfanov](#) (the researcher who came up with the unofficial patch) has come out with a WMF vulnerability checker to allow you to test your systems for the vulnerability.

Another test now exists. This was created by Kevin Gennuso and you can download it [here](#). This file will open Windows Calculator and kill the explorer.exe process on vulnerable systems but otherwise causes no damage.

Be careful about using this on an important system.

Are the number of exploits likely to increase?

Yes. This has been a fast-changing exploit and it's far from over.

Do you have additional links?

Here are a few:

- [SANS Internet Storm Center WMF FAQ](#)
- [Microsoft Technet](#)
- [CERT](#)
- [CVE](#)
- [Sunbelt Blog on the updated patch](#)
- [Security Fix](#)
- [TechBlog](#)

[Download a copy of this document in PDF format \(110kb\)](#) - feel free to distribute.