SANS Internet Storm Center
WMF Vulnerability Briefing

http://isc.sans.org

Outline

- What are WMF Files and what is wrong with them?
- How is the exploit currently used?
- How do I protect myself?
- What should I do if I get infected?

For updates and links to the unofficial patch, see

http://handlers.sans.org/jullrich/wmffaq.html

About the Internet Storm Center

- Cooperative Incidents Response Community
- Volunteer Operated (about 40 ISC Handlers)
- vendor neutral
- operating the largest worldwide sensor network, DShield.org.
- depending on input from readers and volunteers donating a large part of their holiday weekend.

What are WMF Files

- WMF = Windows Meta Files.
- proprietary Microsoft (MSFT) image format.
- Vector file format. Great for shapes/line graphics that need to be scaled. Used frequently in MSFT office applications.
- The image is described by the procedures used to draw the lines/bitmaps.
- WMF Images have the ability to execute system functions.

What is Wrong With WMF Images

- An arbitrary function can be specified as part of the “SETABORTPROC” code.
- **This code will be executed whenever the image is viewed.**
- The 'SETABORTPROC' function was intended to be called if a printing process is aborted.
- The images are parsed by a DLL called “shimgvw.dll”. This DLL will pass the image to gdi32.dll which will execute the code.

Why is this worse then other issues?

- No patch or easy workaround available. (MSFT announced that patch will be available Jan. 10th.)
- Execution of the exploit requires no or minimal user interaction.
- Images are usually considered safe, and users are not afraid to click/view them.
- The vulnerability is being used in the wild for malicious purposes.
- The malicious images are hard to detect as the bad code can hide anywhere in the file.
- Extension doesn't matter. Preview/Icon View triggers Execution. Indexing Programs may trigger execution without user interaction.

How is the exploit used?

- Malicious images are added to compromised web sites.
- Images are sent via Instant Messenger.
- Images are sent via e-mail.
- These malicious images are used to install a wide range of malicious software:
  - backdoors / bots
  - spyware
  - keyloggers
  - adware
  - all of the above

How can I protect myself?

Microsoft is not offering any patches for this issue at this time.

- Unofficial patch, created by Ilfak Guilfanov. This patch has been carefully vetted by ISC handler Tom Liston.

- "Unregister" the affected DLL in order to prevent its execution.

Currently, the unofficial patch and unregistering the DLL is your best bet to prevent an exploit. We strongly recommend doing both!

Why Unregister + Patch ?

- Unregister will remove the DLL which by default parses WMF images.
- But this will not fix the actual vulnerability in GDI32.dll.
- The patch will prevent execution of malicious code by patching the DLL in memory. The actual DLL file is not modified.
- Both steps are required right now to provide the best possible protection.
- Side effects are due to unregistering the shimgvw.dll. Some thumbnail functions in various applications will no longer work.

Other Workarounds

- Firewalls: Typically have limited content inspection ability. However, limiting users to a small list of trusted sites may be an option
- Antivirus: Antivirus vendors are working hard to detect different versions of the exploit. Currently, not all AV vendors are able to detect all versions of the exploit.
- Limited User Accounts: Limited User Accounts can limit the damage caused by the exploit, but will not prevent the exploit
- Data Execution Protection (DEP): Only works if support by your CPU (e.g. AMD64).

Other Workarounds (2)

- Blocking just .WMF images will not work, as the extension is inconsequential. WMF images are recognized by a special “magic header”.
- Using a browser other then Internet Explorer provides little help as the issue is not an MSIE issue.
- Removing the affected DLL works, but has to be done right (after disabling windows file protection).
- Just unregistering the DLL is ok, but it may be re-registered by some software.

What if I get Infected?

- Isolate infected system.
- Follow standard incident handling procedures.
- Call Microsoft support at 1-866-PCSAFETY.
- Many exploits install additional malware.
- Anti Virus software may detect some of the additional malware, but not all of it.
- Complete recovery can be difficult or impossible. Restore from a recent backup is recommended.

Where can I find more details?

- Internet Strom Center: http://isc.sans.org
  - FAQ: http://isc.sans.org/diary.php?storyid=994
  - List of WMF related diaries:

    http://isc.sans.org/diary.php?storyid=993.

- Microsoft: http://www.microsoft.com/technet/security/advisory/912840.mspx

Thanks!

This work could not be done without the numerous contributions from our readers, Ilfak's unofficial patch and not without our ISC handlers!

For current updates, check http://isc.sans.org

Please report any exploit attempts, updates, or additional information to http://isc.sans.org/contact.php