

[VulnWatch] UPDATED: Quick JPEG/GDI test & fix (timesaver)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-10/0006.html>

From: GuidoZ (uberguido_z_at_gmail.com)

Date: 10/07/04

Date: Thu, 7 Oct 2004 10:14:30 -0700

To: vulnwatch@vulnwatch.org

Hello again list,

I've made a small update to the "install" SFX and batch file. It was brought to my attention that the batch file might not work correctly on non-English versions, though it will run. (Thanks Morten/DK*CERT!) I have fixed this. It should now run independent of the Windows language version.

The updated file is in the same place:

– <http://www.guidoz.com/exploit-test.exe>

I'll also take this time to warn you that up-to-date antivirus programs SHOULD and WILL detect this as a virus! I mentioned that it attempts to exploit the system to see if it's vulnerable. It uses an infected JPG to do that – AV programs should be picking this up if they are up-to-date. If you still want to test the exploit, you can disable your AV scanner. (Though, if it's stopping it there, you should be safe.)

Last but not least; many people are asking for the batch files and such separately. I have no problem sharing them at all! The SFX archives were for ease of use. I have the files themselves available for download as ZIP files on my web server. Each zip file contains what the self-extracting EXE (SFX) extracts and runs, along with the SFX itself. You can also open up the SFX file with any compression program (WinRAR is my fav) and freely change and move things around. You can even rename the batch file if you like – just be sure to rename it in the INI file. (That's what the launching program uses to know what to launch.) You should see what I mean when you see the files.

If you use WinRAR, you can freely modify the files, then put them back in by drag-n-drop method. That way you can still use the SFX file which is setup to automatically extract and run the batch file (again, according to the SFX archive). Hopefully that all makes sense. =)

VulnWatch: [VulnWatch] UPDATED: Quick JPEG/GDI test & fix (timesaver)

Here's where to download the files:

Install file I posted to the lists is here:

– <http://www.guidoz.com/install.zip>

The exploited JPEG downloads these files (as an SFX, which is included):

– <http://www.guidoz.com/jpegtest.zip>

Obviously you won't be able to change what file the JPEG downloads unless you create a new "infected" JPEG. There is a program available to do this called "JPEG Downloader". I have also written a batch file to run this safely (without exploiting yourself). Just make sure to put these files in a folder you do NOT have open in Explorer! Run the "makejpg.bat" file from a DOS prompt only.

You can download the JPEG Downloader here:

– <http://www.guidoz.com/makejpg.zip>

If you have other questions, again, please feel free to email:

– exploit_AT_guidoz_DOT_com

--

Peace. ~G