

Full-Disclosure: [Full-Disclosure] Re: Windows XP explorer.exe heap overflow.

[Full-Disclosure] Re: Windows XP explorer.exe heap overflow.

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-02/1343.html>

disclosure_at_ossecurity.ca

Date: 02/24/04

To: <full-disclosure@lists.netsys.com>

Date: Tue, 24 Feb 2004 15:08:53 -0500

We checked both EMF and WMF files out and changed around the sizes and it did not crash Windows XP (SP1, EN). From the posts on the full disclosure, it seems what you reported might be caused by other factors. Or it is exploitable on older version of XP?

Here is a list of modules loaded. XP tested (not crashing): Build 2600
xpsp1.020828-1920; SP1

92 Module: 5cb00000: C:\WINDOWS\System32\shimgvw.dll for
C:\WINDOWS\EXPLORER.EXE

93 Module: 5cb00000: C:\WINDOWS\System32\shimgvw.dll for C:\PROGRAM
FILES\INTERNET EXPLORER\IEXPLORE.EXE

Peter Huang

OSsurance, Protection Against Win32 Viruses and BOF Worms

<http://www.ossecurity.ca/>

> -----Original Message-----

> From: sunglasses@bay-watch.com [mailto:sunglasses@bay-watch.com]

> Sent: Friday, February 20, 2004 1:46 PM

> To: bugtraq@securityfocus.com

> Subject: Windows XP explorer.exe heap overflow.

>

>

>

>

> Vulnerability in XP explorer.exe image loading

> ----- Systems affected:

> Current XP – others not tested. Degree: Arbitrary code

> execution. Summary ----- A malformed .emf (Enhanced Metafile,

> a graphics format) file can cause an exploitable heap overflow in

> (or near) shimgvw.dll. Details ----- The image preview code

> that explorer uses has an exploitable buffer overflow. An .emf

> file with a "total size" field set to less than the header size

> will causes explorer.exe to crash in the heap routines – in

Full-Disclosure: [Full-Disclosure] Re: Windows XP explorer.exe heap overflow.

> classic heap overflow style that should be exploitable a la the
> RPC exploits. There are two overflows here: 1. A buffer is
> allocated with the size indicated in the header (no validity
> checks), then the header is copied into it – if the size is less
> than the header size, that's one overflow. 2. They then proceed
> to read the rest of the file to a length of (size–headersize),
> which allows for an integer overflow causing the rest of the file
> to be appended to the already blown buffer. Exploit ----- To
> exploit this flaw (in explorer), simply place a malformed
> (invalid "size" field) .emf file in any directory, open explorer
> to that path, and view as Thumbnails. Bang. In it's simplest
> form it's a DOS – it affects all explorer windows, including File
> Open dialogs for many programs. Alternatively, without viewing
> as a Thumbnail, open the picture preview window for the .emf
> file. (It's the default double–click action). Using this trigger
> causes a different crash point, which may not be exploitable, but
> I wouldn't rule it out. Additional notes ----- It may
> be worth checking out similar issues in .wmf files, as they are
> similar. – Jellytop, 2004 "If a man will begin with
> certainties, he shall end in doubts; but if he will be content to
> begin with doubts he shall end in certainties."
>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>