

Re: A Very Dangerous Worm in Windows Metafile Images (WMF)

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2006-01/msg00225.html>

- *From:* Rich Grise <richgrise@xxxxxxxxxxx>
 - *Date:* Mon, 02 Jan 2006 17:53:42 GMT
-

On Mon, 02 Jan 2006 06:43:34 -0800, Winfield Hill wrote:

> Frank Bemelman wrote...
>>
>> Winfield Hill wrote...
>>> Pooh Bear wrote...
>>>>
>>>> I suspect that's the case. My Windoze (98SE) is fully patched and
>>>> up to date with all the Microsoft security issue fixes installed.
>>>>
>>>> I 'passed' the current online test for this exploit btw. It's not
>>>> *guaranteed* but helps put my mind at rest.
>>>
>>> I dunno, some sites I read say the test fails to properly see
>>> the vulnerability on Win98. Others point out the WMF hole is
>>> valid back to Windows 3.0 So I'd be very careful.
>>>
>>> I wonder where all this expertise suddenly comes from.
>>>
>>> The only thing that running such online test proves is that there
>>> are still folks around who trust and run software just like that,
>>> on their computers that didn't show any signs of problems ;)
>>>
>>> Now that is worth a 'Sheesh'.
>>>
>>> It did sound dangerous, so I went to a dozen trusted security
>>> sites to see what they recommended, and after seeing each one
>>> say, don't wait, get with it NOW, I acted. And posted here.
>>> I also posted links to a few of the security sites earlier in
>>> this thread, don't trust me, trust the experts on this subject.
>>> E.g., "Trust us," <http://isc.sans.org/diary.php?storyid=996>
>>>
>>> I recommend installing MSDOS 2.0 before it is too late. Joerg
>>> still has copies.
>>>
>>> :--|}

The whole thing could probably be nipped in the bud, and most viruses,

Re: A Very Dangerous Worm in Windows Metafile Images (WMF)

worms, and such, if people could be taught to not do their day-to-day stuff while logged in as administrator, but to create user accounts that don't have permission to install executable programs, and especially that don't have permission to overwrite system files.

Or, run Linux. :-)

Cheers!
Rich

• *Follow-Ups:*

- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Winfield Hill

• *References:*

- ◆ [*A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Mike Monett
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Mike Monett
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: JeffM
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Mike Monett
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Frank Bemelman
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Winfield Hill
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Pooh Bear
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Winfield Hill
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Pooh Bear
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Winfield Hill
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Frank Bemelman
- ◆ [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
◇ From: Winfield Hill

- Prev by Date: [*Re: Digital Current Control for LED array*](#)
- Next by Date: [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
- Previous by thread: [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
- Next by thread: [*Re: A Very Dangerous Worm in Windows Metafile Images \(WMF\)*](#)
- Index(es):
 - ◆ [*Date*](#)

Re: A Very Dangerous Worm in Windows Metafile Images (WMF)

◆ ***Thread***