

microsoft.public.security: Re: Is it safe to open a text file in Internet Explorer?

Re: Is it safe to open a text file in Internet Explorer?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-03/0472.html>

From: Galen (galennews_at_gmail.com)

Date: 03/12/05

Date: Sat, 12 Mar 2005 02:53:14 -0500

In news:%23JG6W4rJFHA.2980@TK2MSFTNGP10.phx.gbl,
Jim Carlock <anonymous@localhost> had this to say:

My reply is at the bottom of your sent message:

- > *Don't bother with the Error 1 stuff or Error 2 stuff there.*
- > *They'll just confuse things.*

I'd already clicked on the link but edited it to go up a level and see what was posted. I'm ALMOST always willing to sacrifice a computer for the cause. ;) (I use Ghost and isolate the PC from the network for such things. Robear probably knew I couldn't resist clicking his link...)

Anyhow, what I'm going to get to here, is this is a flaw...

No doubt about that. It's certainly a flaw and NEEDS to be reported ASAP.

However, the question was, and remains, is this a security risk? I'm going to hope that I have your permission to explore this further. I didn't see any copyright notice and the source is freely available, at any time you can request I not do so if you'd like however. I would honor such requests...

What we're looking at here, if opened in IE, is a potential to include harmful content in a file that's not rendered properly in IE. However, because it's not rendered properly I'm inclined to say, at this point, it is unlikely that anything can be executed from this and thus wouldn't be executed. Safe? Yes. In my opinion! Just MY opinion! Okay? LOL Someone, probably a 14 year old kid living in his parent's basement, is going to come along and exploit this but I don't see that as viable.

What is odd, in the thread from the tinyurl link:

"Download it to your disk, change the extension, then Send To Internet Explorer. With .gif, or .jpg you get a missing picture look. With a .bmp extension you get an error message that it is NOT a bitmap. With .txt you get what you indicated. With

Re: Is it safe to open a text file in Internet Explorer?

microsoft.public.security: Re: Is it safe to open a text file in Internet Explorer?

an .html or .htm extension it appears similar to blank.htm. With an .xml extension you get "The XML page cannot be displayed." "

When I opened the link in IE I got the XML page error:

```
*****  
XML Page cannot be displayed
```

Cannot view XML input using style sheet. Please correct the error and then click the Refresh button, or try again later.

```
*****
```

That was with the .txt extension... The real question is, is this flaw capable of executing an unsafe file? No? I really HATE to give a certain answer here. I've read, re-read, Googled, and MSN searched --- MSN search is getting pretty good by the way --- and I really want to say "NO" but I've always been skeptical. In this case that means that I don't THINK that there's potential for exploitation by NORMAL means for this nor any known at this time. However it needs more research...

IF you do NOT mind there's a few people I'd like to direct to this thread. They are as harmless as I and probably better educated (31 and still haven't finished college and probably never will) and are more likely to be able to spot immediate flaws than I. Also, of note, I've read the works of Matt Gibson and think that he's taken an interest to this thread as well. Yes, I'm like that. Anyhow, I've done a small bit of playing over the past couple of hours while answering email and reading a few others and I don't see a way that this can actually execute anything.

Once again, to repeat what's in the newsgroup thread that this is from, this is WELL worth knowing about and IS a potential problem IF there is a way to make this execute a file. Right now I (I wish that I could bold that I because it's meant to diminish my importance or knowledge and not exemplify it) can't find a way to make it do so. Someone else may very well be able to and while I believe in full disclosure under most circumstances this isn't necessarily one of them. If they do know how to make this do so then they should probably inform someone more important than us here in the newsgroups.

Galen

--
Signature changed for a moment of silence.
Rest well Alex and we'll see you on the other side.