

Re: [Full-disclosure] windows vulnerability? [was: Re: [Code-Crunchers] 137 bytes]

Re: [Full-disclosure] windows vulnerability? [was: Re: [Code-Crunchers] 137 bytes]

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-11/msg00131.html>

- *From:* "Thomas Pollet" <thomas.pollet@xxxxxxxxx>
 - *Date:* Wed, 8 Nov 2006 05:38:06 -0800
-

Hello,

On 08/11/06, Gadi Evron <ge@xxxxxxxxxxxxx> wrote:

On Wed, 8 Nov 2006, onisan wrote:

- > One thing is in this makes it even more interesting, most of the firewalls
- > do not block this download, so it's smallest and most dangerous downloader
- > at the same time :o

What Alex did is very impressive! Matthew Murphy came up with the idea originally, I think, but it doesn't take from this amazing work in any way.

awe struck

I'd say more though, it's a vulnerability.

If you can load a library remotely, and do so with no problems, it's a vulnerability in Windows. I am not sure of what kind quite yet.

Windows handles UNC paths the same way as local paths. Another mechanism used to load a remote dll using a UNC path is described in

<http://opensores.thebunker.net/pub/mirrors/blackhat/presentations/win-usa-04/bh-win-04-litchfield/bh-win-04-litchfield>

here the "system" directory is overwritten with a (unc) directory owned by the attacker. When GetSystemDirectoryW() is called to load the faultrep.dll on exception, an attacker can supply his backdoored faultrep.dll. I don't think you should classify this as a vulnerability, it's known windows behaviour (yet, windows, a vulnerability all by itself?).

Regards,
Thomas

The mother of all downloaders.

Re: [Full-disclosure] windows vulnerability? [was: Re: [Code-Crunchers] 137 bytes]

Re: [Full-disclosure] windows vulnerability? [was: Re: [Code-Crunchers] 137 bytes]

"The Zone has a new King!" <we're not worthy x3>
-- Jeff, Coupling (BBC, UK).

Gadi.

> -- G
>
> 2006/11/8, Solar Eclipse <solareclipse@xxxxxxxxxxxx>:
>>
>> On Tue, Nov 07, 2006 at 10:56:42AM -0800, Peter Ferrie wrote:
>>> Why is the idata size present? AFAIK, no Windows version checks it.

>>> Four bytes shorter, then (stop at the idata rva non-zero byte)?
>>
>> You're right, you can remove the last field and bring the file size
down
>> to 133 bytes. That's what I get for claiming that the size can't be
>> improved :-)
>>
>> Solar
>> _____
>> Code-Crunchers mailing list
>> Code-Crunchers@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> <http://whitestar.linuxbox.org/mailman/listinfo/code-crunchers>

Full-Disclosure - We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia - <http://secunia.com/>