

Re: old netscape vuln – affecting XP/explorer?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-09/0062.html>

From: Peter Andersson (aspersion@jure-divino.com)

Date: 09/08/02

From: "Peter Andersson" <aspersion@jure-divino.com>

To: <vuln-dev@securityfocus.com>

Date: Sun, 8 Sep 2002 22:46:08 +0200

> *Hi*

> *I posted this to bugtraq, but was advised to post here..*

>

> *I d/loaded the old 'crash-netscape.jpg' from secfocus (id 1503,*

>

> <http://online.securityfocus.com/data/vulnerabilities/exploits/crash-netscape.jpg>)

> *Sorry if it wraps*

>

> *intending to have a play with Mozilla ;). I stuck it into my cygwin*

> *dir on my local HD.*

>

> *When I browse to this folder using explorer (**Tiles view**),*

> *I get an explorer restart. (all open explorer windows close, but apps*

> *persist)*

>

<snip>

>*Does anyone else get the same?*

I had a really quick look at the issue and also crashes explorer.exe on my system (Windows XP Pro, all currently available patches for the swedish version 08-Sep).

>*Is this exploitable? – I get the same address (0x0003812) every*

Probably, getting it to work often enough is above my current level of skill though.

>*time...is this adjustable with the header/etc in the dodgy .jpg?*

Re: old netscape vuln – affecting XP/explorer?

SecurityFocus Vuln-Dev: Re: old netscape vuln – affecting XP/explorer?

Yes.

I also saw rundll32.exe crashing if using XP default image viewer for the .jpg format. Although I did not look into the rundll32.exe issue too much, I was unable to adjust any register by changing values in the image file.

However I was able to adjust some register values in the explorer.exe process:

–[FILE]–

At offset 0x00001019:

0xa8 0x54

[0x23 0x22 0x21 0x20]<–These four bytes will be in ecx

[0x13 0x12 0x11 0x10]<–These four bytes will be in eax

0x00 0x00 0x00 0x00 0x00 0x00

–[PROGRAM]–

(7b4.120): Access violation – code c0000005 (first chance)

ntdll!RtlTimeToTimeFields+2b3:

eax=10111213 ecx=20212223

77f52cd0 8908 mov [eax],ecx

This should allow an exploit to write any value to wherever the explorer.exe has write permission (return address on the stack, exception handlers on the stack). I have only looked at this for a very short time so I'm sure someone more resourceful can come up with the POC for this, if the stackpointer would be more consistent it would be straightforward I believe. But I do not have any more time to look at this so I'm sharing what little I have found.

-
- **Previous message:** [Michal Zalewski: "x509 cert parsing in web browsers"](#)
 - **Maybe in reply to:** [cassidy macfarlane: "old netscape vuln – affecting XP/explorer?"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)