

Re: Internet Explorer 6 CSS "expression" Denial of Service Exploit (P.o.C.)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-12/msg00223.html>

- *From:* "chinese soup" <noodle.mastah@xxxxxxxxxx>
 - *Date:* Sat, 9 Dec 2006 22:21:41 +0100
-

Someone pointed out to me my mistake in berrating other people when they were just helping out with the issue that they feel would be helpful, so I apologize to the second poster who tested it on IE7 (since yes, IE7 should be tested as well on these issues. and IMO, IE7 is WAY better than firefox, until at least they fix some issues hehe. yes, the irony.). But for others who wanted to post it for IE6 on a whatever version of Windows, pthooowheey to youu!!!

and, I am still too lazy at figuring out the issue, but it so happens that I looked into my magic-noodle-bowl-of-enlightenment and...

```
<div style="width: expression(window.open(self.location));">
```

in a big booming voice reminiscent of what-other-people-call-GOD (and yes, i was quite shocked to realized that it talked!

"WHAT DOES THE CODE DO, YOUNG GRASSHOPPER?"

grasshopper my ass.

opens poc in IE.

"Ehrm, it opens a new instance of itself in a new window? and each new window opens a new window because it uses the same code? *light-bulb* like those dolls that open up to reveal another doll, although smaller, and THAT opens up to reveal another smaller doll, and that smaller doll opens up again to reveal YET another smaller-than-the-previous-dolls..."

"STOP!!!! BUT YES, YOU ARE SOMEWHAT CORRECT! WHAT HAPPENS IF YOU KEEP ON OPENING WINDOWS, YOUNG GRASSHOPPER?"

*quit it with the grasshopper thing!"

"Hmmm.... I guess the system would run out of memory to create the new window?"

"AND?!?!?!"

stares at noodle bowl.

".... and... probably opening tons of windows consumes memory... and... so... the crash? Just like when you reach the last doll and it doesn't open so you throw it against the wall to break it and see what's inside?"

"NOT VERY WELL SAID, BUT I BELIEVE YOU GET THE IDEA. WELL DONE, YOUNG GRASSHOPPER. ALTHOUGH I WOULD SAY YOU NEED MORE PRACTICE!!!! AND PLEASE, DO NOT USE THE METAL-BRUSH WHEN YOU WASH ME, IT HURTS. NOW GO AND STUDY MORE!"

"Wait!!! now I have questions!!"

"Can this be leveraged to execute code?!?!"

"how come the 'width' field allows some sort of code, and not just arithmetic operations?!?!"

"What about the other PoC's?! You only discussed one!!!"

"LOOK INSIDE YOURSELF!!! USE YOUR eE-nner EYE!!!"

o-keeeey then

enlightened,

"you know why noodles tastes great on a rainy night? it's because the cooks have runny noses. mmmmm"

On 12/8/06, chinese soup <noodle.mastah@xxxxxxxx> wrote:

(waiting for the deluge of other lemmings who go:

"it works on blahblah with SPblahblah"

"confirmed on blahblah with blahblah language"

"blahblah did not work for me blahblah"

can't you just find out the cause and not test EVERY version of IE that you have? I mean, yeah, ok, so you tested it on IE7 yeah big deal. he reports it on IE6.

you know why it is "putting iexplore.exe at 100% CPU"?

It's like when a truck crashes into a car and everyone goes out and tests the truck against their own cars:

"Hey, the truck also totally destroyed my Ford Explorer!"

"Oh, it also totalled my Toyota!".

"Nope, it had no effect on my tank"

yeah i mean i COULD test it, but i'm too busy with... ehm... cooking. yes cooking.

cooking,

"i like my noodles boiled, not fried. well, sometimes fried"

On 12/7/06, Andrius Paurys <andrius.paurys@xxxxxxxx> wrote:

> On 12/6/06, José Carlos Nieto Jarquín <xiam.core@xxxxxxxx> wrote:

Re: Internet Explorer 6 CSS "expression" Denial of Service Exploit (P.o.C.)

>> Note:
>> I'm sorry, two of the the exploits in the prior e-mail were incomplete.
>>
>> This is just another couple of proof of concept exploits for this
>> well-known browser. The third one is a lame combination of both.
>>
>> Tested under Windows XP SP2, MSIE 6.0.2900.2180
>
>
> Also confirmed working on Windows Server 2003 R2 (Build 3790) with
> Internet Explorer 7.0.5730.11
>
> 1st exploit was working fine putting iexplore.exe at 100% CPU. It
> complained about "IE restricting this web page from running scripts"
> (probably because of enabled Internet Explorer Enhanced Security
> Configuration), but if you click "allow this website to run this"
> (which is enabled by default if above mentioned IE ESC is not present)
> it works.
>
> 2nd and 3rd were not exactly working, (also because of IE ESC) because
> after clicking allow after several windows it was asking again, but
> should work on WinXP and IE7.
>
>
>
> --
> Andrius Paurys
> \$h@MAN
>
> andrius.paurys@xxxxxxxxxx
> Tel.: +37067449273
> ICQ: 279424019
> MSN: andrius.paurys@xxxxxxxxxx
> <http://shaman.tinkle.lt/>
>
> I'm Lithuanian, what's _your_ excuse?
> S di programeris nevalg s ir nieko...
>