

Re: incredible

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2004-09/3388.html>

From: John Larkin (jjlarkin_at_highlandSNIPtechTHISnologyPLEASE.com)

Date: 09/16/04

Date: Wed, 15 Sep 2004 18:55:09 -0700

On Thu, 16 Sep 2004 02:25:21 +0200, "Frank Bemelman"
<f.bemelmanx@xs4all.invalid.nl> wrote:

> "John Larkin" <jjlarkin@highSNIPlandTHIStechPLEASEnology.com> schreef in
> bericht news:0fehK0pu2lnsvefnus0i6neroqnie39j5a@4ax.com...
>> On Thu, 16 Sep 2004 07:41:27 +1000, "Adam. Seychell"
>> <invalid@invalid.com> wrote:
>>
>> > Dirk Bruere at Neopax wrote:
>> >
>> >> John Larkin wrote:
>> >>
>> >>> <http://www.securityfocus.com/news/9508>
>> >>>
>> >>
>> >> "The old bromide that promises you can't get a computer virus by
> looking
>> >> at an image file crumbled a bit further Tuesday when Microsoft
> announced
>> >> a critical vulnerability in its software's handling of the ubiquitous
>> >> JPEG graphics format.
>> >>
>> >>> The security hole is a buffer overflow that potentially allows an
>> >>> attacker to craft a special JPEG file that would take control of a
>> >>> victim's machine when the user views it through Internet Explorer,
>> >>> Outlook, Word, and other programs. The poisoned picture could be
>> >>> displayed on a website, sent in e-mail, or circulated on a P2P network.
>> >>
>> >>> Utter incompetence – it really is unbelievable.
>> >>
>> >>
>> >>> I'd like to know the relationship between the buffer overflows and a how
>> >>> its possible to exploit the this bug to create malicious code. Is there
>> >>> some functions in the Microsoft image decoding routines that say if a
>> >>> buffer overflow then execute a undocumented and secret language format
>> >>> imbedded inside JPEG files ? !!!
>> >>

>> > *Can someone please explain what possible like exists between buffer
>> > overflows and computer viruses ? A buffer overflow is nothing more than
>> > an pointer going outside its intended range.
>> > Has anyone seen proof of this vulnerability yet ?
>> >
>> > Adam
>> >
>> >
>> > *It's been done many times. Far too may times.
>> >
>> > Just google "buffer overflow." Or maybe "Microsoft stupidity."
>
> Just google for "buffer overflow linux" and "buffer overflow windows".
> 522.000 hits versus 397.000 ;)
>
> It's not so much MS stupidity, but more a C problem. Functions like
> strcpy, scanf, gets, they are all too much relying on decent input
> that isn't any larger than the reserved buffer. In C++ it is easier
> to protect yourself, but there is enourmous amount of plain C, even
> embedded in C++ classes. The leaks are all over the place ;) Each and
> every classic array declaration is a potential problem.**

It wouldn't be if the operating system enforced I/D space separation,
as was an established practice 30 years ago.

I wonder if OOP makes things worse by mixing code and data so
intimately.

John