

Re: Parameter Overflow Attack?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-11/0718.html>

From: Barry Margolin (barmar@genuity.net)

Date: 11/30/02

From: Barry Margolin <barmar@genuity.net>

Date: Sat, 30 Nov 2002 06:25:33 GMT

In article <20021128223319.220e64dd.spamtrap@flash-gordon.me.uk>,

Mark Gordon <spamtrap@flash-gordon.me.uk> wrote:

> On 28 Nov 2002 19:09:35 GMT

> roberson@ibd.nrc.ca (Walter Roberson) wrote:

>

>> In article <20021128164153.41e80c7b.spamtrap@flash-gordon.me.uk>,

>> Mark Gordon <spamtrap@flash-gordon.me.uk> wrote:

>> :Also, the normal C calling conventions are that the parameters are

>> :pushed on to the stack in reverse order, followed by the return

>> address:so the called routine would see everything correctly. The

>> caller is then:normally responsible for removing the parameters from

>> the stack.

>>

>> I do not think that you are correct that this is

>> "the normal C calling convention".

>

>I did not say normal, I said standard ;-)

Huh? Your message is quoted above, and the third word is "normal".

But if you meant standard, which standard were you talking about? I don't think ISO/ANSI C specifies the way in which arguments are passed, nor do any of the Unix specifications (POSIX, SUS, etc.). This type of detail is generally covered in ABIs, not standards that deal with source code only.

--

Barry Margolin, barmar@genuity.net

Genuity, Woburn, MA

*** DON'T SEND TECHNICAL QUESTIONS DIRECTLY TO ME, post them to newsgroups.

Please DON'T copy followups to me -- I'll assume it wasn't posted to the group.