

Re[2]: SV: Avoiding Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/linuxsecurity/2002-01/0044.html>

From: Trano (Trano@gmx.net)

Date: 01/10/02

Date: Thu, 10 Jan 2002 15:31:36 +0100

From: Trano <Trano@gmx.net>

To: "lists@notatla.demon.co.uk" <security-discuss@linuxsecurity.com>

Sorry, sure you're right, I was a bit confused yesterday and didn't understand what you meant.

thx for the help :)

- > *Polluting the stack with your chosen values does not give you instant*
- > *control of the program. Instead it leaves a value in memory for later use*
- > *that you hope will get you control *when the current function returns*.*

- > *If it never returns because the whole program has exited don't expect to*
- > *see the effect of the overflow. (Not that effect anyway. A function ending*
- > *in exit() might still have vulnerabilities affecting the way data is handled,*
- > *but the traditional attack is to alter the return address.)*

- > *The core dumps often arising from overflows are often because execution*
- > *at 0x41414141 is impossible and a different value needs to be used in*
- > *that part of the overflow string. Beginning with your shellcode in an*
- > *environment variable (as in one of the P49-14 examples) seems simplest*
- > *to me.*

- > *Bruce Schneier in "Secrets and Lies" compares a buffer overflow to a*
- > *delivery man in a shop with dim staff who follow an instruction manual.*
- > *If the delivery man puts a bogus sheet of instructions on the bottom of*
- > *his pile of forms and doesn't take it back again he's managed to transfer*
- > *a sheet of his onto the top of the instruction manual. *Next time the*
- > *shopkeeper consults it* he might find something like "help driver remove*
- > *all beer from shop".*

To unsubscribe email security-discuss-request@linuxsecurity.com
with "unsubscribe" in the subject of the message.

- **Previous message:** [Patrick Duane Dunston: "Re: Setuid and setgid files"](#)
- **In reply to:** lists@notatla.demon.co.uk: "Re: SV: Avoiding Buffer Overflows"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)