

Re: Avoiding Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/linuxsecurity/2002-01/0025.html>

From: Trano (Trano@gmx.net)

Date: 01/08/02

Date: Tue, 8 Jan 2002 23:29:18 +0100

From: Trano <Trano@gmx.net>

To: Dave Wreski <security-discuss@linuxsecurity.com>

Hi there.

That's now a bit off topic from the original question/discussion, but also regarded to buffer overflows and avoiding them.

Someone told me a program like this:

[--snip--]

```
#include <stdio.h>
```

```
int
```

```
main(int argc, char **argv)
```

```
{
```

```
    char buf[100];
```

```
    strcpy(buf, argv[1]);
```

```
    exit(1);
```

```
}
```

[--snip--]

would not be exploitable because of the "exit(1)".

I'm not familiar with C yet so I don't know if he's right or not. I looked for some text which handles this topic but I couldn't find one. Even Smashing the stack for fun and profit doesn't mention this aspect so now I'm confused.

May someone here can tell me what's right :-)

thx a lot

Tom

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

• *Previous message:* [David Correa: "Re: Question about security !!!"](#)

Linux–Security: Re: Avoiding Buffer Overflows

- *In reply to:* Dave Wreski: "Re: Avoiding Buffer Overflows"
- *Next in thread:* David Correa: "Re: Avoiding Buffer Overflows"
- *Reply:* David Correa: "Re: Avoiding Buffer Overflows"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]