

## Re: Privilege-escalation attacks on NT-based Windows are unfixable

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-10/2579.html>

---

*From:*

*Date:* 08/28/02

Date: Tue, 27 Aug 2002 22:00:49 -0400

Edward Elliott wrote:

>  
> *On Tue, 27 Aug 2002 01:27:25 -0400, Douglas A. Gwyn wrote:*  
> >  
> > *It isn't within the charter of these committees. In any event, if you*  
> > *think language features will guarantee security (or program*  
> > *correctness in general), then you haven't learned from previous*  
> > *attempts. And trying to strait-jacket C (to take the most important*  
> > *example) would wreck its use as a systems programming language.*  
>  
> *I'm not saying they should "guarantee" security (as if that were*  
> *possible), just give security-conscious advice. For example,*  
> *recommend elimination of strcpy, strcat,*

With care, these two can be used without chance of buffer overflows.

> *gets,*

IMHO, this atrocity should never have existed :)

> *sprintf,*

Though not quite an atrocity, this shouldn't have existed — it should have been snprintf from the beginning, IMHO.

> *and scanf.*

A line from the man page for fscanf, for what modifiers are allowed:

"An optional non-zero decimal integer that specifies the maximum field width."

If this modifier were \*non\*-optional for the s and [ field specifiers, then (f)scanf would be fairly safe.

> *It doesn't force programmers to program securely, but it does remove*

comp.security.misc: Re: Privilege-escalation attacks on NT-based Windows are unfixable

> *the worst offenders. Likewise, propose a safer string library, which*  
> *has more benefits than just security.*  
>  
> *The idea is that libraries should encourage secure rather than*  
> *insecure programming. There's no need to strait-jacket anyone. I'm*  
> *not saying "make it impossible to write insecure code". As long as*  
> *the application runs on a flawed os, that task is impossible.*  
>  
> > *Tell you what -- you design a "secure programming language" and*  
> > *present it for review.*  
>  
> *I'm not a language designer; I have neither the interest nor the*  
> *education to do this.*

The Perl programming language, with taint checking enabled, comes pretty close to being a secure programming language.

```
--  
tr/^4/ /d, print "@{[map --$| ? ucfirst lc : lc, split]},\n" for  
pack 'u', pack 'H*', 'ab5cf4021bafd28972030972b00a218eb9720000';
```

---

- **Next message:** vivian: "Re: HELP!!!!"
- **Previous message:** Don Saklad: "How to set up EMACS RMAIL for priority correspondents messages."
- **In reply to:** Edward Elliott: "Re: Privilege-escalation attacks on NT-based Windows are unfixable"
- **Next in thread:** :"Re: Privilege-escalation attacks on NT-based Windows are unfixable"
- **Reply:** :"Re: Privilege-escalation attacks on NT-based Windows are unfixable"
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]