

## Re: avoiding stackguard

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-10/0248.html>

---

**From:** Crispin Cowan ([crispin\\_at\\_immunix.com](mailto:crispin_at_immunix.com))

**Date:** 10/22/04

Date: Thu, 21 Oct 2004 16:25:17 -0700

To: [vallez@gmail.com](mailto:vallez@gmail.com)

Vallez appears to be using "stackguard" generically to refer to stack protections. Since the example code provided is for Windows, and (AFAIK) there has never been a StackGuard port to Windows, he is not actually talking about StackGuard per se.

If you mean "StackGuard", then say so. If you mean some kind of generic protection for stacks, then call it something else. "StackGuard" is a registered trademark of Immunix Inc.

Crispin

[vallez@gmail.com](mailto:vallez@gmail.com) wrote:

```
>hi,
>im posting here a manner for avoiding stackguard. Shellcode without zeros.
>
>/*****/
>/*Shellcode avoiding stack protections sample-----Vallez/29a*/
>/*****/
>
>/*
>All we have listened about stack protections. Security products are protecting stacks of code executed there.
New
>hardware too, that will not let you to execute code in a not executable memory (amd64 for example).
>
>Doing shellcodes avoiding this fact is not very complex, as i will show with this small sample.
>
>The idea is to use pieces of code of dlls for example. In this code im using pieces of code of ntdll for doing
my
>purposes. How? Easy, with the stack overflow we will leave in the stack ret addresses for conduction our
thread
>to code in ntdll.dll. Exactly we are using these codes in ntdll:
>
>
>-----
>
>.78462FDF: AB stosd
```

SecurityFocus Bugtraq: Re: avoiding stackguard

>.78462FE0: 5F pop edi  
>.78462FE1: C20400 retm 00004  
>  
>-----  
>  
>.784635EC: 8BC6