

[UNIX] IA32 System Call Emulation Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-09/msg00034.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 25 Sep 2007 10:57:53 +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>

IA32 System Call Emulation Vulnerability

SUMMARY

Insufficient validation of general-purpose register in IA32 system call emulation code may lead to local system compromise on x86_64 platform.

DETAILS

Vulnerable Systems:

- * Linux 2.6
- * Linux 2.4

On x86_64 platform the Linux kernel supports compatibility emulation for IA32 userland applications providing 32-bit system calls amongst other 32-bit resources.

As a result of arch/x86_64/ia32/ia32entry.S code optimization invalid opcodes was used in the low level assembler routines providing insufficient validation of %RAX register in the following part of code (2.6):

```
---8<---  
sysenter_do_call:
```

[UNIX] IA32 System Call Emulation Vulnerability

```
cmpl $(IA32_NR_syscalls-1),%eax
ja ia32_badsys
IA32_ARG_FIXUP 1
call *ia32_sys_call_table(%rax,8)
---8<---
cstar_do_call:
cmpl $IA32_NR_syscalls-1,%eax
ja ia32_badsys
IA32_ARG_FIXUP 1
call *ia32_sys_call_table(%rax,8)
---8<---
ia32_do_syscall:
cmpl $(IA32_NR_syscalls-1),%eax
ja ia32_badsys
IA32_ARG_FIXUP
call *ia32_sys_call_table(%rax,8) # xxx: rip relative
---8<---
```

Improperly validated 64-bit values stored in the %RAX register may lead to out-of-bounds system call table access resulting in the ability to execute arbitrary code in the context of the Linux kernel.

Impact:

Unprivileged local user may execute arbitrary code in the context of the Linux kernel running on x86_64 platform.

Disclosure timeline:

18th September 2007 – Vendor notification
24th September 2007 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:cliph@xxxxxxxxxxxxxxxxxxxxxxxx>>
Wojciech Purczynski.

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

[UNIX] IA32 System Call Emulation Vulnerability

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.