

COSEINC LINUX ADVISORY #2

IA32 System Call Emulation Vulnerability

=== [ABSTRACT] =====

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

=== [AFFECTED SOFTWARE] =====

Linux 2.6
Linux 2.4

For the exact kernel version please refer to information provided by your vendor.

=== [DESCRIPTION] =====

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:
    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

===[**AUTHOR**]=====

Wojciech Purczynski <cliph@research.coseinc.com>

Wojciech Purczynski is a Security Researcher at Vulnerability Research Labs, COSEINC PTE Ltd. Wojciech Purczynski is also a member of iSEC Security Research.

===[**LEGAL DISCLAIMER**]=====

Copyright (c) 2007 Wojciech Purczynski
Copyright (c) 2007 COSEINC PTE Ltd.

All Rights Reserved.

PUBLISHING, DISTRIBUTING, PRINTING, COPYING, SCANNING, DUPLICATING IN ANY FORM, MODIFYING WITHOUT PRIOR WRITTEN PERMISSION IS STRICTLY PROHIBITED.

THE DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. THE CONTENT MAY CHANGE WITHOUT NOTICE. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, INJURIES, LOSSES OR UNLAWFUL OFFENCES.

USE AT YOUR OWN RISK.