

[VulnWatch] COSEINC Linux Advisory #1: Linux Kernel Parent Process Death Signal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-08/msg00005.html>

- *From:* Wojciech Purczynski <cliph@xxxxxxx>
 - *Date:* Tue, 14 Aug 2007 17:17:14 +0200 (CEST)
-

====[ABSTRACT]=====

An unprivileged local user may send arbitrary signal to a child process despite security restrictions.

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

Linux 2.6
Linux 2.4

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

====[DESCRIPTION]=====

Typically unprivileged user can not send signal to processes running with different UID. Due to vulnerability found in the Linux kernel any local user may bypass security restrictions and send arbitrary signal to any child process executed by the user.

When a parent process dies or exits its child processes may receive a signal. Each child process may choose and set its own "parent process death signal" using PR_SET_PDEATHSIG function of the prctl() system call.

PARENT CHILD

fork()
prctl(PR_SET_PDEATHSIG)
exit()'ed or killed
child receives the signal

The parent process death signal is not reset over execve() system call and is inherited by spawned process:

PARENT CHILD

```
fork()
prctl(PR_SET_PDEATHSIG)
execve("./a.out")
exit()'ed or killed
child receives the signal
```

The signal gets delivered only if parent process has sufficient privileges to send signals to child processes. Typically any child process running with higher privilege than its parent will receive no signal.

PARENT CHILD

```
fork()
prctl(PR_SET_PDEATHSIG)
execve("/bin/setuid-binary")
exit()'ed or killed
child receives NO signal this time
```

However, above restriction may be bypassed if parent process execute setuid-root binary which dies afterwards.

PARENT CHILD

```
fork()
prctl(PR_SET_PDEATHSIG)
execve("/bin/setuid-binary")
execve("/bin/setuid-binary")
exit()'ed or killed
privileged process receives the signal
```

===[DISCLOSURE TIMELINE]=====

27th July 2007 Vendor notification
14th August 2007 Public disclosure

===[AUTHOR]=====

Wojciech Purczynski <cliph@xxxxxxxxxxxxxxxxxxxxxx>

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]=====

[VulnWatch] COSEINC Linux Advisory #1: Linux Kernel Parent Process Death Signal Vulnerability

Copyright (c) 2006,2007 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.