# CVE Detail – CVE-2009-3547

Multiple race conditions in fs/pipe.c in the Linux kernel before 2.6.32-rc6 allow local users to cause a denial of service (NULL pointer dereference and system crash) or gain privileges by attempting to open an anonymous pipe via a /proc/\*/fd/ pathname.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.89363

## CVSS Scoring

CVSS v3.1 Score: 7.0

Severity: HIGH

## Mapped CWE(s)

* CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
* CWE-476: NULL Pointer Dereference
* CWE-672: Operation on a Resource after Expiration or Release

## CAPEC(s)

* CAPEC-26: Leveraging Race Conditions
* CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions

## Affected Products

* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.32:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.32:rc1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.32:rc2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.32:rc3:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.32:rc4:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.32:rc5:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:novell:linux\_desktop:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux\_enterprise\_desktop:10:sp2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux\_enterprise\_server:10:sp2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:6.06:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:9.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:9.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vma:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:mrg\_realtime:1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:4.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:5.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*