# CVE Detail – CVE-2009-4895

Race condition in the tty\_fasync function in drivers/char/tty\_io.c in the Linux kernel before 2.6.32.6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via unknown vectors, related to the put\_tty\_queue and \_\_f\_setown functions. NOTE: the vulnerability was addressed in a different way in 2.6.32.9.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.203

## CVSS Scoring

CVSS v3.1 Score: 4.7

Severity: MEDIUM

## Mapped CWE(s)

* CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
* CWE-476: NULL Pointer Dereference

## 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:debian:debian\_linux:5.0:\*:\*:\*:\*:\*:\*:\*
* 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:9.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:9.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:10.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:10.10:\*:\*:\*:\*:\*:\*:\*