# CVE Detail – CVE-2008-4302

fs/splice.c in the splice subsystem in the Linux kernel before 2.6.22.2 does not properly handle a failure of the add\_to\_page\_cache\_lru function, and subsequently attempts to unlock a page that was not locked, which allows local users to cause a denial of service (kernel BUG and system crash), as demonstrated by the fio I/O tool.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.36014

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-667: Improper Locking

## CAPEC(s)

* CAPEC-25: Forced Deadlock
* CAPEC-26: Leveraging Race Conditions
* CAPEC-27: Leveraging Race Conditions via Symbolic Links

## ATT&CK Techniques

* T1499.004: Application or System Exploitation

## Used By (Actors/Tools)

* Industroyer (malware)

## Affected Products

* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:5.0:\*:\*:\*:\*:\*:\*:\*