# CVE Detail – CVE-2009-1961

The inode double locking code in fs/ocfs2/file.c in the Linux kernel 2.6.30 before 2.6.30-rc3, 2.6.27 before 2.6.27.24, 2.6.29 before 2.6.29.4, and possibly other versions down to 2.6.19 allows local users to cause a denial of service (prevention of file creation and removal) via a series of splice system calls that trigger a deadlock between the generic\_file\_splice\_write, splice\_from\_pipe, and ocfs2\_file\_splice\_write functions.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.33825

## CVSS Scoring

CVSS v3.1 Score: 4.7

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:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.30:rc1:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:2.6.30:rc2:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* 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:8.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:9.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:10.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise:11.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_desktop:11:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:11:-:\*:\*:\*:\*:\*:\*