# CVE Detail – CVE-2009-3553

Use-after-free vulnerability in the abstract file-descriptor handling interface in the cupsdDoSelect function in scheduler/select.c in the scheduler in cupsd in CUPS 1.3.7 and 1.3.10 allows remote attackers to cause a denial of service (daemon crash or hang) via a client disconnection during listing of a large number of print jobs, related to improperly maintaining a reference count. NOTE: some of these details are obtained from third party information.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.92623

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-416: Use After Free

## Affected Products

* cpe:2.3:a:apple:cups:1.3.7:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apple:cups:1.3.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:10:\*:\*:\*:\*:\*:\*:\*
* 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:debian:debian\_linux:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:5.0:\*:\*:\*:\*:\*:\*:\*