# CVE Detail – CVE-2009-2692

The Linux kernel 2.6.0 through 2.6.30.4, and 2.4.4 through 2.4.37.4, does not initialize all function pointers for socket operations in proto\_ops structures, which allows local users to trigger a NULL pointer dereference and gain privileges by using mmap to map page zero, placing arbitrary code on this page, and then invoking an unavailable operation, as demonstrated by the sendpage operation (sock\_sendpage function) on a PF\_PPPOX socket.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.94887

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-908: Use of Uninitialized Resource

## Affected Products

* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_real\_time:10:\*:\*:\*:\*:\*:\*:\*
* 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:5.3:\*:\*:\*:\*:\*:\*:\*
* 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\_server\_aus:5.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*