# CVE Detail – CVE-2009-4272

A certain Red Hat patch for net/ipv4/route.c in the Linux kernel 2.6.18 on Red Hat Enterprise Linux (RHEL) 5 allows remote attackers to cause a denial of service (deadlock) via crafted packets that force collisions in the IPv4 routing hash table, and trigger a routing "emergency" in which a hash chain is too long. NOTE: this is related to an issue in the Linux kernel before 2.6.31, when the kernel routing cache is disabled, involving an uninitialized pointer and a panic.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.82034

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## 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:2.6.18:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:virtualization:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:5.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*