# CVE Detail – CVE-2005-2456

Array index overflow in the xfrm\_sk\_policy\_insert function in xfrm\_user.c in Linux kernel 2.6 allows local users to cause a denial of service (oops or deadlock) and possibly execute arbitrary code via a p->dir value that is larger than XFRM\_POLICY\_OUT, which is used as an index in the sock->sk\_policy array.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.31129

## 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:2.6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:3.1:\*:\*:\*:\*:\*:\*:\*