# CVE Detail – CVE-2008-5038

Use-after-free vulnerability in the NetWare Core Protocol (NCP) feature in Novell eDirectory 8.7.3 SP10 before 8.7.3 SP10 FTF1 and 8.8 SP2 for Windows allows remote attackers to cause a denial of service and possibly execute arbitrary code via a sequence of "Get NCP Extension Information By Name" requests that cause one thread to operate on memory after it has been freed in another thread, which triggers memory corruption, aka Novell Bug 373852.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.95057

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-416: Use After Free

## Affected Products

* cpe:2.3:a:novell:edirectory:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp1:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp2:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp3:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp4:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp5:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp6:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp7:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp8:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.7.3:sp9:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:novell:edirectory:8.8:-:\*:\*:\*:windows:\*:\*