# CVE Detail – CVE-2010-0211

The slap\_modrdn2mods function in modrdn.c in OpenLDAP 2.4.22 does not check the return value of a call to the smr\_normalize function, which allows remote attackers to cause a denial of service (segmentation fault) and possibly execute arbitrary code via a modrdn call with an RDN string containing invalid UTF-8 sequences, which triggers a free of an invalid, uninitialized pointer in the slap\_mods\_free function, as demonstrated using the Codenomicon LDAPv3 test suite.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.9733

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-252: Unchecked Return Value

## Affected Products

* cpe:2.3:a:openldap:openldap:2.4.22:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esxi:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esxi:4.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*