# CVE Detail – CVE-2002-1347

Multiple buffer overflows in Cyrus SASL library 2.1.9 and earlier allow remote attackers to cause a denial of service and possibly execute arbitrary code via (1) long inputs during user name canonicalization, (2) characters that need to be escaped during LDAP authentication using saslauthd, or (3) an off-by-one error in the log writer, which does not allocate space for the null character that terminates a string.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.92684

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-131: Incorrect Calculation of Buffer Size

## CAPEC(s)

* CAPEC-100: Overflow Buffers
* CAPEC-47: Buffer Overflow via Parameter Expansion

## Affected Products

* cpe:2.3:a:cyrusimap:cyrus\_sasl:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*