# CVE Detail – CVE-2004-1363

Buffer overflow in extproc in Oracle 10g allows remote attackers to execute arbitrary code via environment variables in the library name, which are expanded after the length check is performed.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.96215

## 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:oracle:application\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.2.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.2.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.2.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.2.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.2.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.3.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:application\_server:9.0.4.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:collaboration\_suite:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:8.1.7.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:9.0.1.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:9.0.1.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:9.0.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:9.2.0.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:9.2.0.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:database\_server:10.1.0.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.6:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.7:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:e-business\_suite:11.5.9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager:9.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_database\_control:10.1.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_grid\_control:10.1.0.2:\*:\*:\*:\*:\*:\*:\*