# CVE Detail – CVE-2008-5748

Directory traversal vulnerability in plugins/spaw2/dialogs/dialog.php in BloofoxCMS 0.3.4 allows remote attackers to read arbitrary files via the (1) lang, (2) theme, and (3) module parameters.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.91445

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## Affected Products

* cpe:2.3:a:bloofox:bloofoxcms:0.3.4:\*:\*:\*:\*:\*:\*:\*