# CVE Detail – CVE-2009-1936

\_functions.php in cpCommerce 1.2.x, possibly including 1.2.9, sends a redirect but does not exit when it is called directly, which allows remote attackers to bypass a protection mechanism to conduct remote file inclusion and directory traversal attacks, execute arbitrary PHP code, or read arbitrary files via the GLOBALS[prefix] parameter, a different vector than CVE-2003-1500.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.87329

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## 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:cpcommerce\_project:cpcommerce:\*:\*:\*:\*:\*:\*:\*:\*