# CVE Detail – CVE-2006-7079

Variable extraction vulnerability in include/common.php in exV2 2.0.4.3 and earlier allows remote attackers to overwrite arbitrary program variables and conduct directory traversal attacks to execute arbitrary code by modifying the $xoopsOption['pagetype'] variable.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.9345

## 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')
* CWE-913: Improper Control of Dynamically-Managed Code Resources

## 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:exv2:content\_management\_system:\*:\*:\*:\*:\*:\*:\*:\*