# CVE Detail – CVE-2004-0940

Buffer overflow in the get\_tag function in mod\_include for Apache 1.3.x to 1.3.32 allows local users who can create SSI documents to execute arbitrary code as the apache user via SSI (XSSI) documents that trigger a length calculation error.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.882

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## 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:apache:http\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:openpkg:openpkg:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:openpkg:openpkg:2.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:openpkg:openpkg:2.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hp:hp-ux:11.00:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hp:hp-ux:11.11:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hp:hp-ux:11.20:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hp:hp-ux:11.22:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:slackware:slackware\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:slackware:slackware\_linux:8.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:slackware:slackware\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:slackware:slackware\_linux:9.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:slackware:slackware\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:slackware:slackware\_linux:current:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:8.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:8.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:9.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:suse\_linux:9.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:trustix:secure\_linux:1.5:\*:\*:\*:\*:\*:\*:\*