# CVE Detail – CVE-2009-0749

Use-after-free vulnerability in the GIFReadNextExtension function in lib/pngxtern/gif/gifread.c in OptiPNG 0.6.2 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a crafted GIF image that causes the realloc function to return a new pointer, which triggers memory corruption when the old pointer is accessed.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.60334

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-416: Use After Free

## Affected Products

* cpe:2.3:a:optipng\_project:optipng:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise:9-11:\*:\*:\*:\*:\*:\*:\*