# CVE Detail – CVE-2006-4434

Use-after-free vulnerability in Sendmail before 8.13.8 allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced. NOTE: the original developer has disputed the severity of this issue, saying "The only denial of service that is possible here is to fill up the disk with core dumps if the OS actually generates different core dumps (which is unlikely)... the bug is in the shutdown code (finis()) which leads directly to exit(3), i.e., the process would terminate anyway, no mail delivery or receiption is affected."

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.91381

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-416: Use After Free

## Affected Products

* cpe:2.3:a:sendmail:sendmail:\*:\*:\*:\*:\*:\*:\*:\*