# CVE Detail – CVE-2014-0160

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1\_both.c and t1\_lib.c, aka the Heartbleed bug.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.99994

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-125: Out-of-bounds Read

## CAPEC(s)

* CAPEC-540: Overread Buffers

## Affected Products

* cpe:2.3:a:openssl:openssl:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:filezilla-project:filezilla\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:application\_processing\_engine\_firmware:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:cp\_1543-1\_firmware:1.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-1500\_firmware:1.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:simatic\_s7-1500t\_firmware:1.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:siemens:elan-8.2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:siemens:wincc\_open\_architecture:3.12:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:intellian:v100\_firmware:1.20:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:intellian:v100\_firmware:1.21:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:intellian:v100\_firmware:1.24:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:intellian:v60\_firmware:1.15:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:intellian:v60\_firmware:1.25:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:micollab:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:micollab:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:micollab:7.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:micollab:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:micollab:7.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:micollab:7.3.0.104:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mitel:mivoice:1.1.2.5:\*:\*:\*:\*:lync:\*:\*
* cpe:2.3:a:mitel:mivoice:1.1.3.3:\*:\*:\*:\*:skype\_for\_business:\*:\*
* cpe:2.3:a:mitel:mivoice:1.2.0.11:\*:\*:\*:\*:skype\_for\_business:\*:\*
* cpe:2.3:a:mitel:mivoice:1.3.2.2:\*:\*:\*:\*:skype\_for\_business:\*:\*
* cpe:2.3:a:mitel:mivoice:1.4.0.102:\*:\*:\*:\*:skype\_for\_business:\*:\*
* cpe:2.3:o:opensuse:opensuse:12.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:13.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:12.04:\*:\*:\*:esm:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:12.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:13.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:19:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:20:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:gluster\_storage:2.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:storage:2.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:redhat:virtualization:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_aus:6.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_eus:6.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_tus:6.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:ricon:s9922l\_firmware:16.10.3\(3794\):\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:broadcom:symantec\_messaging\_gateway:10.6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:broadcom:symantec\_messaging\_gateway:10.6.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:splunk:splunk:\*:\*:\*:\*:enterprise:\*:\*:\*