Security Advisory:

Vulnerability OpenSSL CVE-2014-0160

- **Vulnerability description**

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.

More details can be found at:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

- **Vulnerability exposure**

The impact of the vulnerability depends on the actual OpenSSL version in use.

Radware investigated and can report that:

- The following products are not vulnerable to CVE-2014-0160:
  - Products that do not use the vulnerable OpenSSL versions for any purpose (SSL offloading or management) and in any product platform or version.
    - Alteon Application Switch
    - AppDirector
    - DefensePro
    - LinkProof
    - CID
    - AppXcel
    - APSolute Vision
    - APSolute Insite ManagePro
    - vDirect
    - SIP Director
  - Inflight

- Latest Inflight version, 4.3.0 uses OpenSSL 1.0.1f, but only its decryption routines such as RSA and RC4. Inflight performs only passive capture, thus it does not use any of OpenSSL's connection establishment or TLS heartbeat routines so it is not vulnerable to this problem.
- Management and feeds are Java based and not vulnerable

- The following products were found to be exposed to the vulnerability:
  - FastView version 5.0 and up - A fix is already available. Please contact Radware Technical Support for more details. The software package will be available on Radware's Customer Portal in a few days.

    Older versions are not vulnerable.
  - AppWall version 5.7 and up – Version 5.8.2 that fixes this issue is already available.

    Older versions are not vulnerable.

For any additional questions in regards to this statement, please approach Radware Support.

For details on the supported Open SSL versions per product please see Radware Knowledgebase Article 2390.