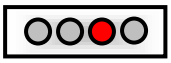
Advanced Notification of OpenSSL-Death-Alert flood remote denial-of-service attack

Security Advisory AE-Advisory 16-040

Criticality High



Advisory Released On 16 November 2016

Impact

Any SSL supported server which uses OpenSSL can be made to deny services through a denial-of-service attack

Solution

Refer to the “Solution” section below

Affected Software

- All OpenSSL versions of 0.9.8
- All OpenSSL versions of 1.0.1
- OpenSSL 1.0.2 through 1.0.2h
- OpenSSL 1.1.0

Not Affected Software

- OpenSSL 1.0.2i, 1.0.2j
- OpenSSL 1.1.0a, 1.1.0b

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new vulnerability in OpenSSL that causes the CPU usage on a server to go up to 100%. Attackers are able to pack multiple alerts inside a single record and send a large number of those records to the server causing it to go into a meaningless cycle and not able to serve any other requests. Further details are explained in the “Threat Details” section below.

Threat Details

The vulnerability's cause is a function called "ssl3_read_bytes" in ssl/s3_pkt.c that leads to higher CPU usage on a server due to its improper handling of warning packets. An attacker is able to repeat the undefined plaintext warning packets of "SSL3_AL_WARNING" during the handshake, which will cause the CPU usage to rise up to 100% on the web server. This is an implementation problem in OpenSSL as it ignores undefined warnings and continues dealing with the remaining data. Once an attacker sends excessively large overlapping alert packets, they are able to cause a Denial-of-Service attack to the server. Fortunately, there is a fix to this problem and it is mentioned in the "Solution" section below.

Solution

- If the version of the OpenSSL on your SSL supported server is mentioned in the "Affected Software" section above, then you will need to upgrade to the latest version of OpenSSL. Please refer to your network administrator for applying this update.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae