CERT-EU

Security Advisory 2022-017

OpenSSL/LibreSSL Vulnerability

March 16, 2022 — v1.0

TLP:WHITE

History:

- *16/03/2022 — v1.0 – Initial publication*

Summary

On March 15th, the OpenSSL project revealed a high severity vulnerability that can lead to Denial-Of-Service for the applications that use certificates from untrusted sources [1]. It can be exploited remotely by an attacker using a specialy crafted certificate that can trigger an infinite loop. LibreSSL was also impacted by this vulnerability and it has been also patched [2].

Technical Details

The `BN_mod_sqrt()` function used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form, contains a bug that can cause the modular square root compute to loop forever for non-prime moduli.

Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters.

Affected Products

This issue affects OpenSSL versions 1.0.2, 1.1.0, 1.1.1 and 3.0.

Respectivelly, it also affects LibreSSL prior to 3.3.6, 3.4.3, and 3.5.1.

Recommendations

- OpenSSL 1.0.2 users should upgrade to 1.0.2zd (premium support customers only)
- OpenSSL 1.1.1 users should upgrade to 1.1.1n
- OpenSSL 3.0 users should upgrade to 3.0.2

OpenSSL 1.1.0 is out of support and no longer receiving updates of any kind. Its users should upgrade to OpenSSL 3.0 or 1.1.1.

Regarding LibreSSL, the patched versions are 3.3.6, 3.4.3, and 3.5.1.

References

[1] https://www.openssl.org/news/secadv/20220315.txt

[2] https://lwn.net/Articles/887972/