CERT-EU

Security Advisory 2023-007

High Severity Vulnerability in OpenSSL

February 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/02/2023 — v1.0 – Initial publication*

Summary

On February 7, the OpenSSL project team has released a major security update to address 8 vulnerabilities. One vulnerability, tracked as **CVE-2023-0286** and rated as **High**, may allow a remote attacker to read arbitrary memory contents or cause OpenSSL to crash, resulting in a denial of service [1].

Technical Details

The `CVE-2023-0286` is a type confusion vulnerability relating to `X.400` address processing inside an `X.509 GeneralName`. When CRL checking is enabled, this vulnerability may allow an attacker to pass arbitrary pointers to a `memcmp` call, enabling them to read memory contents or enact a denial of service.

To exploit the vulnerability, an attacker would need to provide both the certificate chain and CRL, neither of which need to have a valid signature.

This vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

Affected Products

OpenSSL versions 3.0, 1.1.1 and 1.0.2.

Recommendations

CERT-EU recommends applying the available upgrades [1]:

- OpenSSL 3.0 users should upgrade to OpenSSL 3.0.8
- OpenSSL 1.1.1 users should upgrade to OpenSSL 1.1.1t
- OpenSSL 1.0.2 users should upgrade to OpenSSL 1.0.2zg (premium support customers only)

References

[1] https://www.openssl.org/news/secadv/20230207.txt