CERT-EU

Security Advisory 2022-073

OpenSSL High Vulnerabilities

November 1, 2022 — v1.1

TLP:CLEAR

History:

- *27/10/2022 — v1.0 – Initial publication*
- *01/11/2022 — v1.1 – Add technical information*

Summary

On November 1, 2022, the OpenSSL project team has released a new version of the `openssl` library version 3. The version 3.0.7 fixes two HIGH vulnerabilities, `CVE-2022-3602` and `CVE-2022-3786`, that could lead to Denial of Service conditions, or Remote Code Execution in some cases [1]. It is recommended upgrading `openssl` to the last versions.

Proof of concepts are now available. [4]

Technical Details

Originally, the OpenSSL team announced one CRITICAL vulnerability, **CVE-2022-3602**. However, during the week of prenotification, testing and feedback from various organisations showed that the ability to cause remote code execution is really low. Thus, the team decided to downgrade the severity of this CVE to HIGH instead [2].

The second vulnerability, **CVE-2022-3786** was not rated as CRITICAL from the outset, because only the length and not the content of the overwrite is attacker controlled. Exposure to remote code execution is not expected on any platforms [2].

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. This occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer.

In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

The vulnerability **CVE-2022-3786** could be exploited by crafting a malicious email address to overflow an arbitrary number of bytes containing the `.` character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service).

The vulnerability **CVE-2022-3602** could by exploited by crafting a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution depending on stack layout for any given platform/compiler.

Affected Products

- OpenSSL version 3 before 3.0.7.

The vulnerability does not affect OpenSSL versions before 3.0. [2]

Recommendations

CERT-EU recommends upgrading the `openssl` (version 3.x) library to the last version (3.0.7).

As the OpenSSL library is widely used by many third-party applications, many vendors will release updates for their products to fix these vulnerabilities. CERT-EU recommends applying the forthcoming fixes. NCSC-NL, and other partners, are maintaining a non-exhaustive list of products that might be affected, or not, by these vulnerabilities [3].

References

[1] https://www.openssl.org/news/cl30.txt

[2] https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

[3] https://github.com/NCSC-NL/OpenSSL-2022/tree/main/software

[4] https://github.com/DataDog/security-labs-pocs/tree/main/proof-of-concept-exploits/openssl-punycode-vulnerability