Security Bulletin

SecB0006: CVE-2022-3786 AND CVE-2022-3602

Open SSL Vulnerability

Summary

First published: November 16, 2022

Description	An advisory regarding a buffer overflow vulnerability in SSL ver 3.0.7 has been identified and published. In both CVE's a buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking.
Affected Products	N/A
Recommended Action	Enable firewall protection
CVSS v3.X Base Score	7.5 High
CVE ID	CVE-2022-3786 CVE-2022-3602

Description

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate 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). 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.

Security Bulletin

Recommended Action

Users of OpenSSL 3.0.0 - 3.0.6 are encouraged to upgrade to 3.0.7 as soon as possible. If you obtain your copy of OpenSSL from your Operating System vendor or other third party, then you should seek to obtain an updated version from them as soon as possible.

17850 56 Ave Surrey BC Canada V3C 1C7 | Tel: 604.574.9444 | deltacontrols.com

Security Bulletin

Appendix: About CVSS

All CVSS scores can be mapped to the qualitative ratings defined by the Qualitative Severity Rating Scale table (see below):

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. The Base group is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

- The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
- The CVSS v3.0 vector string is a text representation of a set of CVSS metrics. It is commonly used to record or transfer CVSS metric information in a concise form.

For more information, visit the CVSS website at: http://www.first.org/cvss/