PUBLIC

Security Advisory

TBOX-SA-2022-0001

07 November 2022

This security advisory explains why TBox is not affected by OpenSSL CVE-2022-3602 and CVE-2022-3786.

Revision History

Version	Date	Description
1	07/11/2022	Initial Release

1 Executive Summary

- **Document Type**: Security Advisory
- **Reference**: TBOX-SA-2022-0001
- **Vulnerabilities**: CVE-2022-3602 and CVE-2022-3786
- **Severity**: None
- **Publisher**: Ovarro
- **Contact**: cybersecurity@ovarro.com
- **Current Status**: Final
- **Current Version**: 1.0
- **Initial Release Date**: 07 Nov 2022
- **Latest Release Date**: 07 Nov 2022

2 Description

Two vulnerabilities have been discovered in OpenSSL. A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. OpenSSL version 3.0.0 to 3.0.6 are affected.

CVE-2022-3602

CVE-2022-3786

2.1 Affected Products

Ovarro TBox devices use libssl 1.1.1g, which is the portion of OpenSSL which support TLS.

This version of OpenSSL / libssl is not affected by the vulnerabilities.

2.2 Vulnerability Overview

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).

An attacker can craft 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.

2.3 Sources

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

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3786

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3602

3 Mitigating Factors

TBox is not affected.

4 Workarounds

TBox is not affected.