

Xylem Product Security Advisory

Third Party – OpenSSL Vulnerabilities

November 4, 2022

Overview

Two vulnerabilities were released by the OpenSSL Project, which affect OpenSSL software that may be used in select Xylem products.

Xylem is in the process of identifying impacted products along with a remediation approach for affected customers. The status of the affected products is listed within this advisory below.

Vulnerability Details

CVE ID: **CVE-2022-3602** (Severity - High, CVSS Score - TBD)

According to the OpenSSL advisory, the vulnerability could allow a buffer overflow attack resulting in a crash (causing denial of service) on vulnerable systems.

CVE ID: **CVE-2022-3786** (Severity - High, CVSS Score - TBD)

According to the OpenSSL advisory, the vulnerability could allow a buffer overflow attack resulting in a crash (causing denial of service) or potentially remote code execution on vulnerable systems.

Affected Products

Xylem is currently investigating affected products and will update this table as more information becomes available.

Affected Products	Status
In Progress	In Progress

*Xylem products not listed in the above table are not impacted.

Mitigation

In alignment with the guidance from the OpenSSL Project, Xylem strongly recommends affected users take the following actions:

- Upgrade to OpenSSL version 3.0.7

References

- CVE-2022-3602: <https://nvd.nist.gov/vuln/detail/CVE-2022-3602>
- CVE-2022-3786: <https://nvd.nist.gov/vuln/detail/CVE-2022-3786>
- OpenSSL Vulnerabilities: <https://www.openssl.org/news/vulnerabilities.html>
- Xylem: [Product Security Advisories](#)

Contact Information

For any questions related to this Xylem Product Security Advisory, please contact product.security@xylem.com.

Revision History		
Date	Version	Updates
11/4/2022	1.0	Initial Publication

Disclaimer

This document is provided on an as-is basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Use of the information in this document or materials linked from this document is at your own risk. Xylem reserves the right to change or update this document any time.