Xylem Product Security Advisory

Eurotech Everyware Software Framework (ESF) utilized by Xylem Edge Gateway (xGW)

May 26, 2022

Overview

Xylem is aware of a vulnerability that exists in Eurotech's Everyware Software Framework (ESF), which is a third-party software component installed on, and utilized by, the Xylem Edge Gateway (xGW).

Affected Products and Versions

The vulnerability impacts the following software version of Everyware Software Framework (ESF) as used by the Xylem Edge Gateway (xGW):

- Everyware Software Framework (ESF) - Version 6.2.x

Vulnerability Details

Improper Verification of Cryptographic Signature

CVSS v3.0 Base Score 6.7 | **Medium** | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-347: Improper Verification of Cryptographic Signature* vulnerability exists that could allow an attacker to access sensitive information and possibly execute unauthorized code.

Mitigations

In alignment with Eurotech's advisory, Xylem recommends users upgrade to the following versions:

- Everyware Software Framework (ESF) - Version 6.2.2

References

- Xylem Product Security Advisories
- Eurotech Security Advisory

Contact Information

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

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 at any time.

Revision History	
Version	**Updates**
1.0	Initial draft