Xylem Product Security Advisory

AVEVA InduSoft Web Studio Vulnerability for Xylem AquaView

March 16, 2022

Overview

Xylem is aware of a vulnerability that exists in AVEVA's Web Studio platform, which is a third-party component of our legacy AquaView on-premise versions 7.x – 8.1. Mitigation advice is provided in this security advisory.

Affected Products and Versions

The vulnerability impacts the following versions of AquaView on-premise:

- AquaView – Versions 7.x and 8.x, prior to 8.1 SP2

Vulnerability Details

Stack-based Buffer Overflow

CVSS v3.0 Base Score 9.8 | **Critical** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **(Scored by AVEVA)**

A *CWE-121: Stack-based Buffer Overflow* vulnerability exists that could allow a remote attacker to invoke arbitrary processes on the system.

Empty Password in Configuration File

CVSS v3.0 Base Score 9.8 | **Critical** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **(Scored by AVEVA)**

A *CWE-258: Empty Password in Configuration File* vulnerability exists that could allow an unauthenticated remote attacker to make changes to the system.

Mitigations

Xylem recommends users upgrade to AquaView version 8.1 SP2 or greater, or Xylem SCADA On-Premise.

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 the change or update this document any time.