Xylem Product Security Advisory

Xylem Sensus Analytics (SA) Login Service Vulnerability

May 24, 2022

Overview

Xylem identified a vulnerability associated with the password reset capability of the Sensus Analytics (SA) Login Service whereby an unauthorized user may intercept and redirect the reset request to any email address. The vulnerability manifested in two places:

1. When resetting a SA (Utility Portal) password.
2. When changing a SA (Utility Portal) password.

The vulnerability has been remediated, eliminating any impact to the Sensus Analytics solution.

Affected Products and Versions

The vulnerability was related to the Sensus Analytics Login Service of the Utility Portal application.

Vulnerability Details

Improper Authentication

CVSS v3.0 Base Score 7.6 | High | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:N

A *CWE-287: Improper Authentication* vulnerability existed that could have allowed an unauthorized user access to the Sensus Analytics application.

Mitigations

The vulnerability has been remediated. Although there are no reports of any exploits, Xylem recommends resetting your password now.

Xylem recommends Sensus Analytics users reset passwords every three months.

References

- Xylem Product Security Advisories

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.

Revision History	
Version	**Updates**
1.0	Initial draft