Xylem Product Security Advisory

Aanderaa GeoView SQL Injection Vulnerability

November 30, 2021

Overview

Through proactive security testing, Xylem identified an SQL Injection vulnerability that is related to the AADI GeoView Webservice versions prior to version 2.1.3. Xylem is providing mitigation advice in this document.

Vulnerability Details

CVE ID: **CVE-2021-41063**

CVSS v3.0 Base Score 8.2 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

A *CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')* vulnerability exists that could allow an unauthenticated attacker to invoke queries to manipulate the Aanderaa GeoView database server.

Affected Product and Versions

- AADI GeoView Webservice prior to version 2.1.3

Mitigation

Software as a Service (SaaS) / Cloud Users
The vulnerability has been remediated with the implementation of a new production environment in May 2021. The risk to the cloud-based users has been eliminated. Customers are not required to take any further action.

Additionally, Xylem has implemented a defense in depth strategy to reduce the risk of the vulnerability reoccuring including, but not limited to:

- Segmentation of databases and other assets from untrusted networks.
- Deployment of a Web Application Firewall (WAF) solution, configured to block SQL Injection attempts.
- Enforcement of secure system configuration in alignment with best practice.
- Central logging of system events including WAF.

On-Premise Users
Xylem recommends on-premise users to upgrade to AADI GeoView Webservice version 2.1.3.

Please contact Aanderra support at aadi.support@xylem.com for assistance with upgrading to AADI GeoView Webservice version 2.1.3.

References

- Xylem Product Security Advisories
- CVE-2021-41063: NIST National Vulnerability Database (NVD) and MITRE CVE® List
- ICSA-21-334-01 - CISA ICS-CERT 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 on the document or materials linked from the document is at your own risk. Xylem reserves the right the change or update this document any time.