DATE: 03/14/2023

SECURITY BULLETIN AVEVA-2023-002

Title
AVEVA™ Plant SCADA and AVEVA™ Telemetry Server: Improper Authorization

Rating
Critical

Published By
AVEVA Product Security Response Center

Overview
AVEVA Software, LLC. (“AVEVA”) has created a security update to address vulnerabilities impacting:

- AVEVA Plant SCADA 2023, AVEVA Plant SCADA 2020R2 Update 10 and all prior versions (formerly Citect SCADA)
- AVEVA Telemetry Server 2020 R2 SP1 and all prior versions

Vulnerability Technical Details

1. Improper Authorization

The vulnerability, if exploited, could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states.

CWE-285: Improper Authorization
CVSSv3.1: **9.8 Critical** | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-1256

Recommendations
AVEVA recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation. Customers using affected products should apply security updates as soon as possible.

Security Update Downloads

AVEVA Plant SCADA

- All affected versions currently in mainstream support can be fixed by upgrading to AVEVA Plant SCADA 2023 Update 1 or later:
  https://softwaresupportsp.aveva.com/#/producthub/details?id=a145b006-e73d-44d5-9299-08dadcec1ff5
- AVEVA Plant SCADA 2020R2 can alternatively be patched with AVEVA Plant SCADA 2020R2 Update 11 or later:
  https://softwaresupportsp.aveva.com/#/producthub/details?id=8ad9833a-cc4e-4d45-9298-08dadcec1ff5

For additional upgrade information, please refer to the AVEVA Plant SCADA upgrade guide:
https://gcsresource.aveva.com/plantscada/WebHelp/plantscada2023/Content/Upgrading.html

Note: fixes for these vulnerabilities on older versions are not available.

AVEVA Telemetry Server

- All affected versions currently in mainstream support can be fixed by upgrading to AVEVA Telemetry Server 2020 R2 SP2 or later:
  https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=4bbbab19-b1b2-4b0d-ba12-08dafa4ad12d

Note: fixes for these vulnerabilities on older versions are not available.

Acknowledgements

AVEVA would like to thank:

- **UK's National Cyber Security Centre (NCSC)** for discovery and responsible disclosure
- **CISA** for coordination of Advisories

Support

For information on how to reach AVEVA support for your product, please refer to this link: AVEVA Customer Support.
If you discover errors or omissions in this Security Notification, please report the finding to Support.

AVEVA Security Central

For the latest security information and security updates, please visit Security Central.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3.1)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3.1) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3.1 produces a numerical score as well as a textual representation of that score reflecting the severity of a vulnerability. Scores range from 0.0 (no impact) to a maximum of 10.0 (critical impact with minimal effort to exploit). For additional information please refer to the CVSS v3.1 specifications.

Coordination with Authorities

Organizations observing suspected malicious activity should follow established internal procedures and report findings to applicable authorities for tracking and correlation against other incidents.

Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND. AVEVA AND ITS AFFILIATES, PARENT AND SUBSIDIARIES DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY AVEVA, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.
AVEVA DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER'S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN AVEVA DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.
IN NO EVENT WILL AVEVA OR ITS SUPPLIERS, DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF AVEVA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. AVEVA LIABILITY FOR DAMAGES AND EXPENSES HEREUNDER OR RELATING HERETO (WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE) WILL IN NO EVENT EXCEED THE AMOUNT OF ONE HUNDRED DOLLARS ($100 USD).