DATE: 08/13/2024

SECURITY BULLETIN AVEVA-2024-006

Title
AVEVA Reports for Operations: Multiple Vulnerabilities

Rating
High

Published By
AVEVA Product Security Response Center

Overview
AVEVA Group Limited on behalf of itself and its subsidiaries (“AVEVA”) is releasing a security update with fixes to vulnerabilities provided by an upstream software vendor. AVEVA Reports for Operations 2023 and all prior versions are affected by the vulnerabilities.

Vulnerability Technical Details
1. Path Traversal leading to Arbitrary Code Execution
The vulnerability, if exploited, could allow a miscreant to execute arbitrary code under the privileges of an interactive AVEVA Reports for Operations user.

CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
CVSSv4.0: 8.5 High | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CVSSv3.1: 7.8 High | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2024-6618

2. Overriding critical files
The vulnerability, if exploited, could allow a miscreant to read and write an AVEVA Reports for Operations project and/or tamper with installation files.

CWE-732: Incorrect Permission Assignment for Critical Resource
CVSSv4.0: 8.5 High | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CVSSv3.1: 7.8 High | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2024-6619

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

Security Update Downloads

AVEVA Reports for Operations

- All affected versions can be fixed by upgrading to AVEVA Reports for Operations 2023 R2 or higher:

  https://softwaresupportsp.aveva.com/#/producthub/details?id=247ce8d6-0f2e-498c-9024-58c96bb6d8de

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Audit file and folder Access Control Lists for AVEVA Reports for Operations installation and project files to ensure access is limited only to intended users.
- Establish procedures for AVEVA Reports for Operations users to verify the source of projects shared with them is trusted before opening and executing.

Acknowledgements

AVEVA would like to thank:

- **Team82** from **Claroty** for the discovery and responsible disclosure of this vulnerability
- **Ocean Data Systems** (upstream vendor)
- **CISA** for coordination of advisories and generation of CVEs

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 AVEVA security information and security updates, please visit AVEVA Security Central.

U.S. Department of Commerce Industrial Control Systems Security Guide

For general information regarding how to secure Industrial Control Systems please reference the NIST Guide to Operational Technology (OT) Security, NIST SP800-82r3.

NVD Common Vulnerability Scoring System (CVSS v4.0)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v4.0) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v4.0 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 v4.0 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).