DATE: 11/11/2025

SECURITY BULLETIN AVEVA-2025-006

Title
AVEVA Edge (formerly InduSoft Web Studio): Use of Risky Hashing Algorithms

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 to address vulnerabilities impacting:

- AVEVA Edge (formerly InduSoft Web Studio) 2023 R2 and all prior versions.

Vulnerability Technical Details
1. Passwords hashed with MD5
The vulnerability, if exploited, could allow a miscreant with read access to Edge Project files or Edge Offline Cache files to reverse engineer Edge users' app-native or Active Directory passwords through computational brute-forcing of weak hashes.

CWE-327: Use of a Broken or Risky Cryptographic Algorithm
CVSSv4.0: **8.3 High** | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N
CVSSv3.1: **8.4 High** | AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
CVE-2025-9317

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 and affected AVEVA Edge project files should take the following actions to mitigate the risk of exploit:

- Apply AVEVA Edge 2023 R2 P01 Security Update and migrate old project files.
- For projects that cannot be migrated (e.g. backups or transient copies), evaluate the risk of potential password leakage from these files and implement stricter read access controls to protect these unsafe files.
- Require AVEVA Edge users to change their passwords.

Important: Edge project migration from older versions to 2023 R2 P01 is one-way due to the change in password hashing algorithms.

Security Update Downloads

AVEVA Edge

- AVEVA Edge 2023 R2 P01 and higher addresses this vulnerability.

  https://softwaresupportsp.aveva.com/en-US/downloads/products/details/38f52447-3013-4c4e-be6e-9b28b635bba9

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Access Control Lists should be applied to all folders where users will save and load project files.
- Maintain a trusted chain-of-custody on project files during creation, modification, distribution, backups, and use.
- Apply data-protection at the project level with a strong master password. For configuration step-by-step refer to AVEVA Edge “Technical Reference Manual” > Project Overview > Configuring Additional Project Settings > Options Tab > Data Protection.
- If passwords are being used as function parameters inside project documents (such as scripts or worksheets), it is recommended to remove those passwords and use project tags instead. For more information on tags refer to AVEVA Edge “Technical Reference Manual” > Tags and the Tag Database > About Tags and the Project Database.

Acknowledgements

AVEVA would like to thank:

- **João Varelas** for the discovery, coordinated disclosure of this vulnerability with AVEVA, and testing the fix in AVEVA’s Security Update.
- **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).