

Forum:[Hack Forums](#)

Thread: [AVEVA Edge](#)

Stanley - November 29, 2025, 12:05 am

AVEVA Edge

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 8.3

ATTENTION: Low attack complexity

Vendor: AVEVA

Equipment: Edge

Vulnerability: Use of a Broken or Risky Cryptographic Algorithm

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow a local attacker to reverse engineer passwords through brute force.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of AVEVA Edge (formerly InduSoft Web Studio), a HMI/SCADA software, are affected:

Edge: Versions 2023 R2 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 USE OF A BROKEN OR RISKY CRYPTOGRAPHIC ALGORITHM CWE-327

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.

CVE-2025-9317 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.4 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).

A CVSS v4 score has also been calculated for CVE-2025-9317. A base score of 8.3 has been calculated; the CVSS vector string is (AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: United Kingdom

3.4 RESEARCHER

Joao Varelas reported this vulnerability to CISA.

4. MITIGATIONS

AVEVA recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

Users using the affected product versions 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.

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, 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.

For information on how to reach AVEVA support for your product, please refer to this link: [AVEVA Customer Support](#).

For more information, see AVEVA's Security Bulletin AVEVA-2025-006 or AVEVA's bulletins page. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

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

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social

engineering attacks.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time. This vulnerability is not exploitable remotely.

5. UPDATE HISTORY

November 13, 2025: Initial Republication of AVEVA-2025-006

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-03>