DATE: 06/10/2025

SECURITY BULLETIN AVEVA-2025-003

Title
AVEVA PI Web API: Cross Site Scripting Vulnerability

Rating
Medium

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:

- PI Web API, version 2023 SP1 and all prior.

Vulnerability Technical Details
1. Cross Site Scripting
The vulnerability, if exploited, could allow an authenticated miscreant (with privileges to create/update annotations or upload media files) to persist arbitrary JavaScript code that will be executed by users who were socially engineered to disable Content Security Policy protections while rendering annotation attachments from within a web browser.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CVSSv4.0: **4.5 Medium** | AV:N/AC:H/AT:N/PR:L/UI:A/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N
CVSSv3.1: **6.5 Medium** | AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:L/A:N
CVE-2025-2745

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 to mitigate the risk of exploit.

Security Update Downloads
PI Web API

- Upgrade to PI Web API 2023 SP1 Patch 1 or higher:

  From OSISoft Customer Portal, search for "PI Web API" and select version 2023 SP1 Patch 1 or higher.

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Review and update the file extensions allowlist for Annotation attachments to remove potentially vulnerable or undesired file types (ex: svg, pdf, …): https://docs.aveva.com/bundle/pi-server-f-af-pse/page/1022248.html
- Consider implementing IT policies that would prevent users from subverting/disabling Content Security Policy browser protections.
- Inform PI Web API users that Annotation attachments should be retrieved through direct REST requests to PI Web API rather than rendering them in the browser interface.
- Audit assigned privileges to ensure that only trusted users are given “Annotate” access rights: https://docs.aveva.com/bundle/pi-server-f-af-pse/page/1020021.html

Acknowledgements

AVEVA would like to thank:

- **CISA** for coordination of advisories and generation of CVEs

The issues in this alert were self-discovered and self-reported in accordance with OSIsoft’s Ethical Disclosure Policy to inform administrators of potential risks, so that they can take actions to minimize the effects of the vulnerability.

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).