

Forum:[Hack Forums](#)

Thread: [AVEVA PI Web API](#)

Stanley - June 26, 2025, 3:20 am

AVEVA PI Web API

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 4.5

ATTENTION: Exploitable remotely

Vendor: AVEVA

Equipment: PI Web API

Vulnerability: Cross-site Scripting

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to disable content security policy protections.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of AVEVA PI Web API are affected:

PI Web API: Versions 2023 SP1 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION

('CROSS-SITE SCRIPTING') CWE-79

A cross-site scripting vulnerability exists in PI Web API version 2023 SP1 and prior that, if exploited, could allow an authenticated attacker (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.

CVE-2025-2745 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.5 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:L/A:N).

A CVSS v4 score has also been calculated for CVE-2025-2745. A base score of 4.5 has been calculated; the CVSS vector string is

(CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:A/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: United Kingdom

3.4 RESEARCHER

AVEVA Ethical Disclosure reported this vulnerability to CISA.

4. MITIGATIONS

AVEVA recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation. Users of affected product versions should apply security updates to mitigate the risk of exploit.

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

AVEVA further recommends users follow general defensive measures:

Review and update the file extensions allowlist for annotation attachments to remove potentially vulnerable of undesired file types (ex: svg, pdf, ...).

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.

For additional information please refer to AVEVA-2025-003.

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 has a high attack complexity.

5. UPDATE HISTORY

June 12, 2025: Initial Publication

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-08>