

Forum:[Hack Forums](#)

Thread: [AVEVA PI Data Archive](#)

Stanley - February 23, 2026, 7:35 pm

AVEVA PI Data Archive

View CSAF

Summary

Successful exploitation of this vulnerability could result in a denial-of-service condition.
The following versions of AVEVA PI Data Archive are affected:

- PI Data Archive PI Server <=2018_SP3_Patch_7 (CVE-2026-1507)
- PI Data Archive PI Server 2023 (CVE-2026-1507)
- PI Data Archive PI Server 2023_Patch_1 (CVE-2026-1507)
- PI Data Archive PI Server 2024 (CVE-2026-1507)

CVSS

Vendor

Equipment

Vulnerabilities

v3 7.5

AVEVA

AVEVA PI Data Archive

Uncaught Exception

Background

Critical Infrastructure Sectors: Critical Manufacturing
Countries/Areas Deployed: Worldwide
Company Headquarters Location: United Kingdom

Vulnerabilities

Expand All +

CVE-2026-1507

The affected products are vulnerable to an uncaught exception that could allow an unauthenticated attacker to remotely crash core PI services resulting in a denial of service.
View CVE Details

Affected Products
AVEVA PI Data Archive

Vendor:AVEVA
Product Version:AVEVA PI Data Archive PI Server: <=2018_SP3_Patch_7, AVEVA PI Data Archive PI Server: 2023, AVEVA PI Data Archive PI Server: 2023_Patch_1, AVEVA PI Data Archive PI Server: 2024
Product Status:known_affected

Remediations
MitigationAVEVA recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation. Users of affected product versions should apply security updates to mitigate the risk of exploit.
MitigationAll impacted versions of PI Data Archive can be fixed by upgrading to PI Server 2024 R2 or later available here:
<https://softwaresupportsp.aveva.com/en-US/downloads/products/details/8c9b0e8c-eb68-481f-b420-c87a253a4172>.
MitigationPI Data Archive delivered by PI Server 2018 SP3 Patch 7 and prior can be fixed by upgrading to PI Server 2018 SP3 Patch 8 or higher available here:
<https://softwaresupportsp.aveva.com/en-US/downloads/products/details/79492560-7e4c-4800-8bd7-40cce61a17d2>.
MitigationThe following general defensive measures are recommended:
MitigationMonitor liveness of services listed in your installation's "\PI\adm\pisrvstart.bat".
MitigationSet the PI Data Archive Subsystem services to automatically restart.
MitigationPI Data Archive nodes should limit port 5450 inbound access to trusted workstations, users, and software.
MitigationFor additional information please refer to AVEVA-2026-002(
https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2026-002.pdf).

Relevant CWE: CWE-248 Uncaught Exception

Metrics

CVSS Version
Base Score
Base Severity
Vector String

3.1
7.5
HIGH

Acknowledgments

AVEVA reported this vulnerability to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

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](https://www.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](https://www.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.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

Revision History

Initial Release Date: 2026-02-10

Date
Revision

Summary

2026-02-10

1

Initial Republication of AVEVA-2026-002

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-041-03>