AVEVA Pipeline Simulation Missing Authorization

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5387
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 16:16:39 UTC
Updated	2026-04-17 15:09:46 UTC
Description	The vulnerability, if exploited, could allow an unauthenticated miscreant to perform operations intended only for Simulator Ir

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000540000 probability, percentile 0.169140000 (date 2026-04-21)

Problem Types: CWE-862 | CWE-862 CWE-862

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AVEVA	Pipeline Simulation 2025	affected 2025 SP1 (build 7.1.9497.6351) custom	Not specified

References

Reference	Source	Link
softwaresupportsp.aveva.com/en-US/downloads/products/details/57b79fdb-7b5f-4125-8a44-833b...	ics-cert@hq.dhs.gov	softwaresupport
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-10...	ics-cert@hq.dhs.gov	github.com
www.cisa.gov/news-events/ics-advisories/icsa-26-106-04	ics-cert@hq.dhs.gov	www.cisa.gov
www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Se...	ics-cert@hq.dhs.gov	www.aveva.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: All affected versions can be fixed by upgrading to AVEVA Pipeline Simulation 2025 SP1 P01 (build 7.1.9580.8513) or higher: https://softwaresupportsp.aveva.com/en-US/downloads/products/details/57b79fdb-7b5f-4125-8a44-833b6b5c6d6f

Workarounds

CNA: 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.

CNA: The following general defensive measures are recommended: • Restrict Network Access: Implement host-based and/or network firewall controls on all nodes hosting the Pipeline Simulation Server API to ensure that only trusted Pipeline Simulation client systems are permitted to establish connections. • Enforce Secure Communication: Enable TLS for all API communications and ensure that server certificates are properly managed and protected to reduce the risk of manipulator-in-the-middle (MitM) attacks and tampering with data in transit.

There are currently no legacy QID mappings associated with this CVE.