DATE: 06/11/2024

SECURITY BULLETIN AVEVA-2024-003

Title
PI Web API: Remote Code Execution due to Deserialization of Untrusted data vulnerability

Rating
High

Published By
AVEVA Product Security Response Center

Overview
AVEVA Group Limited on behalf of itself and its subsidiaries ("AVEVA") has created a security update to address vulnerabilities in PI Web API 2023 and all prior.

Vulnerability Technical Details
1. Remote Code Execution due to insecure serialization
The vulnerability, if exploited, could allow malicious code to execute on the PI Web API environment under the privileges of an interactive user that was socially engineered to use API XML import functionality with content supplied by a miscreant.

CWE-502: Deserialization of Untrusted Data
CVSSv3.1: **7.6 High** | AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L
CVE-2024-3468

Recommendations
AVEVA recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation. Customers using affected products should apply security updates as soon as possible.

Defensive Measures and General Considerations
The following general defensive measures are recommended:

- Set "DisableWrites" configuration setting to true if this instance of PI Web API is used only for reading data or GET requests.
- Uninstall Core Endpoints feature if this instance of PI Web API is used only for data collection from AVEVA Adapters. Keep OMF feature installed.
- Limit AF Servers' Administrators, so that most of the PI Web API user accounts don't have the permission to change the backend AF servers.

Impact and severity of vulnerabilities may be reduced through industry accepted IT practices. OSIsoft technical support provides guidance on architectural approaches, backup procedures, network defences, and operating system configuration.

For a starting point on PI System security best practices, see knowledge base article KB00833 - Seven best practices for securing your PI Server.

This alert was published 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.

Security Update Downloads

PI Web API

- (Recommended) All affected versions can be fixed by upgrading to PI Web API 2023 SP1 or later:

  From OSI Soft Customer Portal, search for "PI Web API" and select version "2023 SP1" or later.

- (Alternative) PI Web API 2021 SP3 can be fixed by upgrading PI AF Client to one of the versions specified in Security Bulletin AVEVA-2024-004.

Acknowledgements

AVEVA would like to thank:

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

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 v3.1)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3.1) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3.1 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 v3.1 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).