DATE: 01/18/2024

SECURITY BULLETIN AVEVA-2024-001

Title

AVEVA™ PI Server: Denial of Service vulnerabilities

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 impacting AVEVA PI Server versions:

- 2023
- 2018 SP3 P05 and all prior

Vulnerability Technical Details

1. Denial of Service due to crash

The vulnerability, if exploited, could allow an unauthenticated user to remotely crash the PI Message Subsystem of a PI Server, resulting in denial of service.

CWE-703: Improper Check or Handling of Exceptional Conditions
CVSSv3.1: **7.5 High** | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2023-34348

2. Denial of Service due to memory leak

The vulnerability, if exploited, could allow an unauthenticated user to cause the PI Message Subsystem of a PI Server to consume available memory resulting in throttled processing of new PI Data Archive events and partial denial of service.

CWE-772: Missing Release of Resource after Effective Lifetime
CVSSv3.1: **5.3 Medium** | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CVE-2023-31274

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 defensive measures are recommended:

- Set the PI Message Subsystem to auto restart.
- Monitor the Memory usage of the PI Message Subsystem.
- Limit network access to port 5450 to trusted workstations and software.

  Confirm that only authorized users have access to write to the PI Server Message Log. This is done through configuration of the PIMSGSS entry within the Database Security plugin accessible through PI System Management Tools.

For a list of PI System firewall port requirements, see knowledge base article KB01162 - Firewall Port Requirements.

Impact and severity of vulnerabilities can be reduced through industry accepted IT practices. Please consult your IT engineer for advice on how to best implement these firewall restrictions in your organization's architecture. 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

AVEVA PI Server

- (Recommended) All affected versions can be fixed by upgrading to AVEVA PI Server version 2023 Patch 1 or later:

  From OSI Soft Customer Portal, search for “PI Server” and select version “2023 Patch 1”
- (Alternative) AVEVA PI Server 2018 SP3 Patch 5 and prior can be fixed by deploying AVEVA PI Server version 2018 SP3 Patch 6 or later:

  From OSI Soft Customer Portal, search for “PI Server” and select version “2018 SP3 Patch 6”

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).