DATE: 08/12/2025

SECURITY BULLETIN AVEVA-2025-004

Title
AVEVA PI Integrator for Business Analytics: Arbitrary File Upload and Sensitive Data Exposure

Rating
High

Published By
AVEVA Product Security Response Center

Overview
AVEVA Group Limited on behalf of itself and its subsidiaries ("AVEVA") is releasing a security update to address vulnerabilities impacting:

- PI Integrator for Business Analytics, version 2020 R2 SP1 and all prior.

Vulnerability Technical Details
1. Arbitrary File Upload with potential for code execution
The vulnerability, if exploited, could allow an authenticated miscreant (with privileges to create or access publication targets of type Text File or HDFS) to upload and persist files which may potentially be executed.

CWE-434: Unrestricted Upload of File with Dangerous Type
CVSSv4.0: **7.1 High** | AV:N/AC:L/AT:P/PR:L/UI:A/VC:N/VI:H/VA:L/SC:H/SI:H/SA:H
CVSSv3.1: **7.6 High** | AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:L
CVE-2025-54460

2. Sensitive Data Exposure
The vulnerability, if exploited, could allow an authenticated miscreant (with privileges to access publication targets) to retrieve sensitive information that could then be used to gain additional access to downstream resources.

CWE-201: Insertion of Sensitive Information into Sent Data
CVSSv4.0: **7.1 High** | AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSv3.1: **6.5 Med** | AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVE-2025-41415

Recommendations

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.

Security Update Downloads

PI Integrator for Business Analytics

- Upgrade to PI Integrator for Business Analytics 2020 R2 SP2 or higher:

  From OSISoft Customer Portal, search for "PI Integrator for Business Analytics" and select version 2020 R2 SP2 or higher.

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Audit assigned permissions to ensure that only trusted users are given access rights to publication targets: https://docs.aveva.com/bundle/pi-integrator-for-business-analytics/page/1013185.html
- Ensure publication targets of type Text File or HDFS are configured to limit allowed output file extensions and limit output folders to be logically isolated from critical system components or executable paths:
  - https://docs.aveva.com/bundle/pi-integrator-for-business-analytics/page/1023019.html
  - https://docs.aveva.com/bundle/pi-integrator-for-business-analytics/page/1023009.html
- Consider applying Windows Defender Application Control (WDAC) to prevent execution of unauthorized executables: https://learn.microsoft.com/en-us/intune/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

Acknowledgements

AVEVA would like to thank:

- **Maxime Escourbiac, Michelin CERT,** and **Adam Bertrand, Abicom for Michelin CERT** for the discovery and responsible disclosure of these vulnerabilities to AVEVA.
- **CISA** for coordination of advisories and generation of CVEs

The issues in this alert are self-reported 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.

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 v4.0)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v4.0) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v4.0 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 v4.0 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).