DATE: 08/13/2026

SECURITY BULLETIN AVEVA-2026-005

Title
AVEVA Enterprise SCADA: Unsafe Deserialization

Rating
Medium

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:

- AVEVA Enterprise SCADA version 2025
- AVEVA Enterprise SCADA versions 2024 through 2024 SP1 P01 (inclusive)
- AVEVA Enterprise SCADA versions 2023 through 2023 SP1 (inclusive)
- AVEVA Enterprise SCADA versions 2022 through 2022 SP2 P2 (inclusive)
- AVEVA Enterprise SCADA version 2021 SP2 P5 and all prior versions
- AVEVA Enterprise SCADA HMI versions 2024 and 2024 R2
- AVEVA Enterprise SCADA HMI version 2023 P1 and all prior versions

Vulnerability Technical Details
1. Unsafe Deserialization with potential for code execution
The vulnerability, if exploited, could allow an authenticated miscreant with "DNA Authority – Operator" privilege to tamper with serialized data, potentially resulting in code execution during deserialization under the privilege of Enterprise SCADA security group "DNA Apps".

CWE-502: Deserialization of Untrusted Data
CVSSv4.0: **6.1 Med** | AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N
CVE-2025-7639

Recommendations
AVEVA recommends that customers using affected product versions should perform the following to mitigate the risk of exploit:

1. Evaluate the impact of these vulnerabilities based on your operational environment, architecture, and product implementation.

© 2026 AVEVA Group Limited or its subsidiaries. All rights reserved.

2. Plan an upgrade of Servers and Clients to one of the available fixed versions listed in section “Security Updates”.
3. Configure Servers and Clients as described in section “Apply Secure Serialization Settings”.

Security Updates

Please contact your AVEVA Technical Support representative, Customer Success Manager, Account Manager, or Solution Integrator to obtain the security update best applicable to the product version currently deployed in your environment:

Servers:

- AVEVA Enterprise SCADA v2025 P1 or higher
- AVEVA Enterprise SCADA v2024 SP1 P2
- AVEVA Enterprise SCADA v2023 SP1 P1
- AVEVA Enterprise SCADA v2022 SP2 P3
- AVEVA Enterprise SCADA v2021 SP2 P6
- AVEVA Pipeline Operations for Gas/Liquids v2025 P1 or higher
- AVEVA Pipeline Operations for Gas/Liquids v2024 SP1 P2
- AVEVA Pipeline Operations for Gas/Liquids v2023 SP1 P1
- AVEVA Pipeline Operations for Gas/Liquids v2022 SP2 P3
- AVEVA Pipeline Operations for Gas/Liquids v2021 SP2 P6

Clients:

- AVEVA Enterprise SCADA HMI v2024 R2 HF7 or higher
- AVEVA Enterprise SCADA HMI v2024 P1
- AVEVA Enterprise SCADA HMI v2023 P2 HF1
- AVEVA Pipeline Integrity Monitor (delivered on Pipeline Simulation media) v2025 SP1 P2 or higher
- AVEVA Pipeline Training Simulator (delivered on Pipeline Simulation media) v2025 SP1 P2 or higher
- Measurement Advisor 2025 P1 or higher
- Measurement Advisor 2021 SP1 HF16

Apply Secure Serialization Settings

To fully mitigate the risk of exploit, the following configuration changes must be implemented after all server and client nodes have been upgraded to compatible versions that support the fix:

© 2026 AVEVA Group Limited or its subsidiaries. All rights reserved.

Server Components:

- Change “BinarySerializer” -> “Mode” setting from ‘Binary Formatter’ to ‘Json’.
- Change “BinarySerializer” -> “AcceptBinaryFormattedData” setting from ‘true’ to ‘false’.
- Re-cache the XOS Event Handlers assembly

Client Components:

- Configure clients/products that interface with Enterprise SCADA to only use JSON serialization.

HMI:

- Migrate HMI displays

For step-by-step instructions on where and how to apply these configuration settings, how to migrate HMI displays, compatible server-client versions list, and additional details please refer to KB117814 “AVEVA Midstream Product Bulletin – Removal of Binary Formatter”.

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Audit devices, network topology, and perimeter defences to ensure all applicable security best practices from AVEVA’s Enterprise SCADA Reference System Architecture are adhered to.
- Audit assigned permissions to ensure that only trusted users are given “DNA Authority – Operator” rights: https://docs.aveva.com/bundle/scada-ent-2025/page/651008.html
- Disallow BLT Test clients in production environments.

For additional details on defensive measures, please refer to Section 5 of KB117814 “AVEVA Midstream Product Bulletin – Removal of Binary Formatter”.

Acknowledgements

AVEVA would like to thank:

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

© 2026 AVEVA Group Limited or its subsidiaries. All rights reserved.

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).

© 2026 AVEVA Group Limited or its subsidiaries. All rights reserved.