

SECURITY BULLETIN AVEVA-2026-001

Title

AVEVA Process Optimization (formerly ROMeO): Multiple Vulnerabilities

Rating

Critical

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 Process Optimization (formerly ROMeO) 2024.1 and all prior versions

Vulnerability Technical Details

1. Remote Code Execution through API

The vulnerability, if exploited, could allow an unauthenticated miscreant to achieve remote code execution under OS System privileges of “taoimr” service, potentially resulting in complete compromise of the Model Application Server.

CWE-94: Improper Control of Generation of Code ('Code Injection')

CVSSv4.0: **10.0 Critical** | AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CVE-2025-61937

2. Code Injection through macro functionality

The vulnerability, if exploited, could allow an authenticated miscreant (OS Standard User) to tamper with TCL Macro scripts and escalate privileges to OS System, potentially resulting in complete compromise of the Model Application Server.

CWE-94: Improper Control of Generation of Code ('Code Injection')

CVSSv4.0: **9.3 Critical** | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:H
CVE-2025-64691

3. SQL Injection

The vulnerability, if exploited, could allow an authenticated miscreant (Process Optimization Standard User) to tamper with queries in Captive Historian and achieve code execution under SQL Server administrative privileges, potentially resulting in complete compromise of the SQL Server.

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVSSv4.0: **9.3 Critical** | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:H
CVE-2025-61943

4. Privilege escalation via DLL Hijacking

The vulnerability, if exploited, could allow an authenticated miscreant (OS Standard User) to trick Process Optimization services into loading arbitrary code and escalate privileges to OS System, potentially resulting in complete compromise of the Model Application Server.

CWE-427: Uncontrolled Search Path Element

CVSSv4.0: **9.3 Critical** | AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CVE-2025-65118

5. Privilege escalation via project tampering due to missing ACLs

The vulnerability, if exploited, could allow an authenticated miscreant (OS Standard User) to tamper with Process Optimization project files, embed code, and escalate their privileges to the identity of a victim user who subsequently interacts with the project files.

CWE-862: Missing Authorization

CVSSv4.0: **8.6 High** | AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:L/SC:H/SI:H/SA:H
CVE-2025-64729

6. Malicious Content Delivery via Embedded OLE Objects

The vulnerability, if exploited, could allow an authenticated miscreant (Process Optimization Designer User) to embed OLE objects into graphics, and escalate their privileges to the identity of a victim user who subsequently interacts with the graphical elements.

CWE-676: Use of Potentially Dangerous Function

CVSSv4.0: **8.5 High** | AV:L/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:N/SC:H/SI:H/SA:H
CVE-2025-65117

7. Cleartext transmission of sensitive information

The Process Optimization application suite leverages connection channels/protocols that by-default are not encrypted and could become subject to hijacking or data leakage in certain Man-in-the-Middle or passive inspection scenarios.

CWE-319: Cleartext Transmission of Sensitive Information

CVSSv4.0: **7.6 High** | AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N
CVE-2025-64769

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 Updates

AVEVA Process Optimization (formerly ROMEo):

- All affected versions can be fixed by upgrading to AVEVA Process Optimization 2025 or higher:
<https://softwaresupportsp.aveva.com/en-US/downloads/products/details/a643eaa3-0d85-4fde-ac11-5239e87a68ea>

Defensive Measures and General Considerations

The following general defensive measures are recommended as a temporary measure until the security patch can be installed:

- Apply Host and/or Network firewall rules restricting the taoimr service to accept traffic only from trusted source(s). By default, AVEVA Process Optimization listens on port 8888/8889(TLS). Please refer to the AVEVA Process Optimization Installation Guide for additional details on ports configuration.
- Apply ACLs to the installation and data folders, limiting write-access to trusted users only.
- Maintain a trusted chain-of-custody on Process Optimization project files during creation, modification, distribution, backups, and use.

Acknowledgements

AVEVA would like to thank:

- **Christopher Wu from Veracode** for discovering these vulnerabilities as part of a planned, AVEVA-sponsored penetration test engagement.
- **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 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).