DATE: 08/13/2024

SECURITY BULLETIN AVEVA-2024-007

Title
AVEVA SuiteLink: Denial of Service Vulnerability

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 in SuiteLink Server. Impact is limited only to nodes where SuiteLink Server is installed, as part of the following combinations of product versions and distribution media:

- SuiteLink 3.7.0 and all prior versions, distributed standalone
- AVEVA Historian 2023 R2 P01 and all prior versions, distributed on AVEVA System Platform media
- AVEVA InTouch 2023 R2 P01 and all prior versions, distributed on AVEVA System Platform media
- Application Server 2023 R2 P01 and all prior versions, distributed on AVEVA System Platform media
- AVEVA Communication Drivers Pack 2023 R2 and all prior versions, distributed standalone or on AVEVA System Platform media
- Batch Management 2023 and all prior versions

To confirm whether a node has SuiteLink Server installation, please check the existence of file "wwsls.dll" in \Program Files (x86)\Common Files\ArchestrA folder.

SuiteLink Clients are not affected by this vulnerability and do not need to be patched.

Vulnerability Technical Details
1. Denial of Service (volumetric)
The vulnerability, if exploited, could cause a SuiteLink server to consume excessive system resources and slow down processing of Data I/O for the duration of the attack.

CWE-770: Allocation of Resources Without Limits or Throttling
CVSSv4.0: 8.7 High | AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CVSSv3.1: 7.5 High | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2024-7113

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 as soon as possible.

Security Update Downloads

(Recommended) All impacted products and affected versions can be fixed by installing SuiteLink 3.7.100:

https://softwaresupportsp.aveva.com/#/producthub/details?id=afeb5492-f764-4af3-b408-acc4c991f699

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Apply Host and/or Network firewall rules restricting the SuiteLink server to accept traffic only from trusted source(s). By default, SuiteLink listens on port 5413.

Acknowledgements

AVEVA would like to thank:

- **Idaho National Laboratory as part of US DOE CESER's CyTRICS program** for the discovery and responsible disclosure of this vulnerability
- **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).