DATE: 08/13/2024

SECURITY BULLETIN AVEVA-2024-005

Title
AVEVA Historian: SQL Injection vulnerability in Historian Server

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 AVEVA Historian Server. Historian is distributed on AVEVA System Platform media. Impact is limited only to nodes where Historian Server is installed and the following versions:

- Historian 2023 R2
- Historian 2023 through 2023 P03
- Historian 2020 R2 through 2020 R2 SP1 P01

Vulnerability Technical Details

1. SQL Injection
The vulnerability, if exploited, could allow a malicious SQL command to execute under the privileges of an interactive Historian REST Interface user who had been socially engineered by a miscreant into opening a specially crafted URL.

CWE-89: Improper neutralization of special elements used in a SQL Command ('SQL Injection')
CVSSv4.0: 8.5 High | AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
CVSSv3.1: 8.1 High | AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
CVE-2024-6456

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

Historian is upgraded by AVEVA System Platform media:

- **(Recommended)** All affected versions can be fixed by upgrading to AVEVA System Platform 2023 R2 P01:

  https://softwaresupportsp.aveva.com/#/producthub/details?id=f9477c62-1966-4020-8909-fa20f4ef2b2b

- (Alternative 1) Historian 2023 through 2023 P03 can be fixed by upgrading to AVEVA System Platform 2023 P04

  https://softwaresupportsp.aveva.com/#/producthub/details?id=2a9cc3c1-be8a-4f61-8973-dadab079f9a7

- (Alternative 2) Historian 2020 R2 through 2020 R2 SP1 P01 can be fixed by first upgrading to AVEVA System Platform 2020 R2 SP1 P01 and then applying Hotfix 3190476

  Please contact AVEVA Global Customer Support for instructions on how to download and apply this Hotfix.

Defensive Measures and General Considerations

The following general defensive measures are recommended:

- Establish procedures for Historian REST Interface users to verify the source of URLs shared with them is trusted before opening.

Acknowledgements

AVEVA would like to thank:

- **Maurizio Gatti** from **Accenture S.p.A** 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).