DATE: 03/14/2023

SECURITY BULLETIN AVEVA-2023-001

Title

AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere: Multiple Vulnerabilities

Rating

Critical

Published By

AVEVA Product Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has created a security update to address vulnerabilities impacting:

- AVEVA InTouch Access Anywhere 2023 and all prior versions. InTouch Access Anywhere is delivered as both a standalone install and as an optional sub-feature of AVEVA System Platform.
- AVEVA Plant SCADA Access Anywhere 2020 R2 and all prior versions (formerly Citect Anywhere)

Vulnerability Technical Details

1. Outdated OpenSSL

OpenSSL versions prior to 1.1.1q are susceptible to vulnerabilities that could cause arbitrary code execution and/or denial of service. OpenSSL vulnerability and release note logs can be found here:
https://www.openssl.org/news/vulnerabilities-1.1.1.html
Highest CVSSv3.1: **9.8 Critical** | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Highest CVE-2021-3711

2. Path Traversal

The vulnerability, if exploited, could allow an unauthenticated user to remotely read arbitrary files from the system on which these products are running, resulting in information disclosure.
Public functional exploit code that can target this vulnerability exists.

CWE-23: Relative Path Traversal
CVSS v3.1: **7.5 High** | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2022-23854

3. Outdated jQuery

jQuery versions prior to 3.5.0 are susceptible to multiple vulnerabilities. Jquery changelogs:
https://blog.jquery.com/category/jquery/
Highest CVSSv3.1: **6.1 Medium** | AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Highest CVE-2020-11022

Recommendations

AVEVA recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation. Customers using affected products should apply security updates as soon as possible.

In addition to applying security updates, the following general precautions should be taken to harden the Access Anywhere Secure Gateway service:

- Apply firewall rules to reduce network exposure

Security Update Downloads

AVEVA InTouch Access Anywhere

- All affected versions currently in mainstream support can be fixed by uninstalling the old version and then installing AVEVA InTouch Access Anywhere 2023b or later:
  https://softwaresupportsp.aveva.com/#/producthub/details?id=d848918b-c3c3-489d-e439-08dace3d2997

  Note: Hot-fixes for these vulnerabilities on older versions are not available.

AVEVA Plant SCADA Access Anywhere

- All affected versions currently in mainstream support can be fixed by uninstalling the old version and then installing AVEVA Plant SCADA Access Anywhere 2023 or later:
  https://softwaresupportsp.aveva.com/#/producthub/details?id=ddbc4aa0-f607-4226-8625-08dabdf803e9

  Note: Hot-fixes for these vulnerabilities on older versions are not available.

Acknowledgements

AVEVA would like to thank:

- **Jens Regel of CRISEC** for discovery and responsible disclosure of CVE-2022-23854
- Open-Source Communities for the continued jQuery and OpenSSL library maintenance
- **CISA** for coordination of Advisories

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 security information and security updates, please visit Security Central.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3.1)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3.1) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3.1 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 v3.1 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).