DATE: 05/09/2022

SECURITY ADVISORY AVEVA-2022-001

Title

AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere – Escape from streamed app into OS context

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) is advising customers that certain Windows Operating System functionality when enabled and used in combination with AVEVA™ InTouch Access Anywhere (all versions) and AVEVA™ Plant SCADA Access Anywhere (all versions, formerly known as AVEVA Citect Anywhere and Schneider Electric Citect Anywhere) could result in a vulnerability. The vulnerability, if exploited, would allow an authenticated user to escape from the context of the streamed application (AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere) into the OS and launch arbitrary OS commands. This vulnerability does not result in elevation of privilege as the commands are executed under the security context of the authenticated user that is escaping the application.

Background

Windows OS can be configured to overlay a “Language Bar” on top of any application. When this OS functionality is enabled, the OS Language Bar UI will be viewable in the browser alongside the InTouch Access Anywhere and Plant SCADA Access Anywhere applications. It is possible to abuse the Windows OS Language Bar to launch an OS Command Prompt, resulting in a context-escape from application into OS.

Mitigation Steps

AVEVA recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

Customers using the affected AVEVA products should:

- Disable the Windows Language Bar on the server machine hosting InTouch Access Anywhere and Plant SCADA Access Anywhere applications, unless it is required for corporate policy
- Create unique user accounts with minimal privileges dedicated only to remote access of InTouch Access Anywhere and Plant SCADA Access Anywhere applications.
- Utilize OS Group Policy Objects (GPO) to further restrict what those unique user accounts are allowed to do.
- Restrict access based on Microsoft’s recommended block list: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Vulnerability Characterization and CVSSv3 Rating

AVEVA™ InTouch Access Anywhere and AVEVA™ Plant SCADA Access Anywhere application escape to OS:
CWE-668 Exposure of Resource to Wrong Sphere
7.4 | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

Acknowledgements

AVEVA would like to thank:

- **Giovanni Delvecchio from Aceaspa** for the discovery and responsible disclosure of this vulnerability
- **ICS-Cert** for coordination of advisories

Support

For information on how to reach AVEVA support for your product, please refer to this link: AVEVA Software Global 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)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3 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 CVSSv3.1 specifications.

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).