Date: 11/19/2018

AVEVA Security Advisory LFSEC00000134

Title

Vijeo Citect and Citect SCADA affected by DLL Hijacking vulnerability in a 3rd party component

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has become aware of a vulnerability in a 3rd party component used within the following products:

- **Vijeo Citect™ v7.40**
- **Vijeo Citect 2015**
- **Citect SCADA v7.40**
- **Citect SCADA 2015**
- **Citect SCADA 2016**

The vulnerability, if exploited, could result in Local Code Execution.

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

Vulnerability Details, Characterization, and CVSSv3 Rating

The vulnerability exists in **Schneider Electric Software Update utility versions prior to v2.2.0**. Please refer to SEVD-2018-298-01 and CVE-2018-7799 for further details.

Recommendations

AVEVA recommends all customers using the above listed affected software packages to download and upgrade to the latest version of the Schneider Electric Software Update (SESU) software.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin:

Schneider Electric Software Updates v2.2.0, https://www.update.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_220/SESU_2.2.0_setup_sfx.exe

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 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).