



## **AVEVA Security Advisory LFSEC00000136**

### **Title**

Vijeo Citect and CitectSCADA Vulnerability - Insecure Credentials Storage

### **Rating**

Medium

### **Published By**

AVEVA Software Security Response Center

---

### **Overview**

AVEVA Software, LLC. ("AVEVA") is publishing this advisory to inform customers of a security vulnerability in **Vijeo Citect 7.30 and 7.40** and **CitectSCADA 7.30 and 7.40 versions**. The vulnerability, if exploited, could allow a malicious entity to obtain the Citect User Credentials.

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

### **Recommendations**

Customers using **Vijeo Citect 7.30 and 7.40** and **CitectSCADA 7.30 and 7.40 versions** are affected and should upgrade to **CitectSCADA 2018** as soon as possible.

Customers on **CitectSCADA 7.20 and earlier versions**, as well as **Vijeo Citect 2015, CitectSCADA 2015, and later versions**, are not affected but should upgrade to **CitectSCADA 2018** to receive the latest product improvements.

### **Vulnerability Details**

The Citect User Credentials in memory are stored in clear text. An unauthorized user with high privileges could read the memory and obtain the credentials.

### **Security Updates**

Customers should upgrade to the latest release of **CitectSCADA 2018**.



## Affected Products, Components, and Corrective Security Patches

The following table identifies the currently supported products affected. Software updates can be downloaded from the Global Customer Support “Software Download” area or from the links below:

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
Vijeo Citect 7.30 and 7.40 CitectSCADA 7.30 and 7.40	Multiple	Confidentiality	Medium	<a href="https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=51141">https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=51141</a>

## Vulnerability Characterization and CVSSv3 Rating

[CWE-522](#): Insufficiently Protected Credentials

- Vijeo Citect 7.40 and CitectSCADA 7.40:  
6.5 | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

## Acknowledgements

AVEVA would like to thank:

- **VAPT Team, C3i Center, IIT Kanpur, India** 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 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).