Date: 10/15/2019

AVEVA Security Bulletin LFSEC00000139

Title

IEC870IP Driver for Vijeo Citect and Citect SCADA Vulnerability: Stack-based Buffer Overflow

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) is publishing this bulletin to inform customers of a security vulnerability in the **IEC870IP driver v4.14.02 and earlier for Vijeo Citect and Citect SCADA**. The vulnerability, if exploited, could allow a buffer overflow to occur.

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

Recommendations

Vijeo Citect and Citect SCADA customers using the IEC870IP driver v4.14.02 and earlier are affected and should upgrade to the IEC870IP driver v4.15.00 as soon as possible. This vulnerability impacts only the IEC870IP driver and not the core Vijeo Citect or Citect SCADA software. As a result, an upgrade of the Vijeo Citect or Citect SCADA version is not necessary.

The IEC870IP protocol does not provide for authentication and its use should be evaluated. For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

Vulnerability Details

The IEC870IP driver for Vijeo Citect and Citect SCADA has a buffer overflow that could cause a server-side crash.

Security Updates

Vijeo Citect and Citect SCADA customers using the IEC870IP driver should upgrade to the IEC870IP driver v4.15.00.

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:

Affected Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
IEC870IP driver v4.14.02 and earlier for Vijeo Citect and Citect SCADA	Multiple	Availability	High	**IEC870IP driver v4.15.00** https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=52869

Vulnerability Characterization and CVSSv3 Rating

CWE-121: Stack-based Buffer Overflow

- IEC870IP Driver for Vijeo Citect and Citect SCADA:
  7.5 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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