Date: 07/20/2018

AVEVA Security Bulletin LFSEC00000126

Title

InTouch Access Anywhere Insecure 3rd Party Library usage

Rating

Medium

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has created a security update to address an outdated and insecure 3rd party library used in:

- **InTouch Access Anywhere 2017 Update 2 and older**

The vulnerability, if exploited, could result in a Cross-Site Scripting injection and execution.

Recommendations

Customers using **InTouch Access Anywhere 2017 Update 2 or older** are affected and should upgrade to **InTouch Access Anywhere 2017 Update 2b**.

Vulnerability Details, Characterization, and CVSSv3 Rating

The vulnerability exists in jQuery v2.1.4, a 3rd party open source library used by InTouch Access Anywhere. Please refer to jQuery CVE-2015-9251 for further details.

Security Update

The following Security Update addresses the vulnerabilities outlined in this Security Bulletin:
July 20, 2018: InTouch Access Anywhere 2017 Update 2b
Software Security Update Download:
https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5061

Acknowledgements

AVEVA would like to thank:

- **Google's Security Team** for the discovery, responsible disclosure, and verification of the fix.
- **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