Date: 03/18/2019

AVEVA Security Bulletin LFSEC00000131

Title

InduSoft Web Studio and InTouch Edge HMI - Insecure 3rd Party Component

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AVEVA Software, LLC ("AVEVA") has created a security update to address an outdated and insecure 3rd party component used in:

- **InduSoft Web Studio versions prior to 8.1 SP3**
- **InTouch Edge HMI (formerly InTouch Machine Edition) versions prior to 2017 Update 3**

The vulnerability in the 3rd party component could result in code execution but requires privileged, local access to the user's desktop or the ability to copy files into InduSoft Web Studio or InTouch Edge HMI program folder.

Recommendations

Customers are strongly advised to upgrade to:

- **InduSoft Web Studio v8.1 SP3**
  http://download.indusoft.com/81.3.0/IWS81.3.0.zip
- **InTouch Edge HMI 2017 Update 3**
  https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=52354

Customers who cannot upgrade to the latest version of InduSoft Web Studio or InTouch Edge HMI, can alternatively apply Security Update LFSec131 located at:
http://www.indusoft.com/download/patches/security/LFSec131.zip
https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=52410

Vulnerability Details, Characterization, and CVSSv3 Rating

The vulnerability exists in Gemalto Sentinel Ultra Pro v1.3.2 and older, a 3rd party component used by InduSoft Web Studio and InTouch Edge HMI. Please refer to Gemalto CVE-2019-6534.
AVEVA CVSSv3: 6.5 AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

Acknowledgements

AVEVA would like to thank:

- **Yu Qiang** for responsibly disclosing this vulnerability to ICS-CERT
- **Gemalto** for the quick turnaround of a 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 and InduSoft 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 and InduSoft Security Updates.

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