Date: 02/04/2019

AVEVA Security Bulletin LFSEC00000133

Title

InduSoft Web Studio and InTouch Edge HMI – Remote Code Execution Vulnerabilities

Rating

Critical

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC (“AVEVA”) has released a new version of InduSoft Web Studio and InTouch Edge HMI which includes a security update to address vulnerabilities in **all versions prior to**:

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

The vulnerabilities in the TCP/IP Server Task could allow an unauthenticated user to remotely execute an arbitrary process using a specially crafted database connection configuration file. If the TCP/IP Server Task is disabled, InduSoft Web Studio or InTouch Edge HMI is not vulnerable.

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

Recommendations

Customers are advised to upgrade to:

- **InduSoft Web Studio v8.1 SP3**
- **InTouch Edge HMI 2017 Update 3**

Vulnerability Details

An unauthenticated remote user could use a specially crafted database connection configuration file to execute an arbitrary process on the Server Machine. The code would be executed under the privileges of the InduSoft Web Studio or InTouch Edge HMI runtime and could lead to a compromise of the InduSoft Web Studio or InTouch Edge HMI server machine.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin. 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
InduSoft Web Studio prior to v8.1 SP3	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	http://download.indusoft.com/81.3.0/IWS81.3.0.zip
InTouch Edge HMI prior to 2017 Update 3	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=52354

Vulnerability Characterization and CVSSv3 Rating

CWE-306: Missing Authentication for Critical Function,

CWE-99: Improper Control of Resource Identifiers ('Resource Injection')

- InduSoft Web Studio and InTouch Edge HMI:

  9.8 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Acknowledgements

AVEVA would like to thank:

- **Tenable Research** for the discovery, responsible disclosure of this vulnerability, and testing of the patch
- **ICS-Cert** for coordination of advisories

Support

For information on how to reach AVEVA support for your product, please refer to these links: 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