Date: 10/30/2018

AVEVA Security Bulletin LFSEC00000130

Title

InduSoft Web Studio and InTouch Edge HMI (formerly InTouch Machine Edition) – Remote Code Execution Vulnerabilities

Rating

Critical

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created a security update to address vulnerabilities in:

- **InduSoft Web Studio versions prior to 8.1 SP2**
- **InTouch Edge HMI (formerly InTouch Machine Edition) versions prior to 2017 SP2**

The vulnerabilities in the TCP/IP Server Task could allow an unauthenticated user to remotely execute code with the same privileges as that of the InduSoft Web Studio or InTouch Edge HMI (formerly InTouch Machine Edition) runtime. If the TCP/IP Server Task is disabled, InduSoft Web Studio is not vulnerable.

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

Vulnerability Details

A remote user could send a carefully crafted packet to exploit a stack-based buffer overflow vulnerability during tag, alarm, or event related actions such as read and write, with potential for code to be executed. If InduSoft Web Studio remote communication security was not enabled, or a password was left blank, a remote user could send a carefully crafted packet to invoke an arbitrary process, with potential for code to be executed. The code would be executed under the privileges of the InduSoft Web Studio or InTouch Edge HMI (formerly InTouch Machine Edition) runtime and could lead to a compromise of the InduSoft Web Studio or InTouch Edge HMI (formerly InTouch Machine Edition) server machine.

Recommendations

Customers should upgrade to **InduSoft Web Studio v8.1 SP2** and **InTouch Edge HMI (formerly InTouch Machine Edition) 2017 SP2** as soon as possible.

To identify which version of InduSoft Web Studio or InTouch Machine Edition you have installed:

- Windows Desktop or Server operating system: Navigate to Windows Programs and Features, locate the “InduSoft Web Studio” or “InTouch Machine Edition” entries to review the displayed installed version.
- On a Windows Embedded operating system: navigate to the Bin folder in the installation location of InduSoft Web Studio or InTouch Machine Edition and open the file “CEView.ini”. The installed version can be observed from the “version=*.*.*” attribute within the file.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin.

InduSoft Web Studio v8.1 SP2
InTouch Edge HMI (formerly InTouch Machine Edition) 2017 SP2

New Security Features and Recommendations

Starting with InduSoft Web Studio v8.1 SP2 and InTouch Edge HMI v2017 SP2, the new project wizard will create projects with security enabled by default. AVEVA strongly recommends that customers update existing projects to enable the security features of InduSoft Web Studio and InTouch Edge HMI:

1. Enable the new encrypted channel for communication and disable the unencrypted channel.
2. Set a strong Master Project password.
3. Set a strong password for the built-in account. By default, the built-in account is named Guest.
4. Set strong passwords for all other non-built-in accounts.

Security Patches

All prior versions of InduSoft Web Studio and InTouch Edge HMI are 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
InduSoft Web Studio prior to v8.1 SP2	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	http://download.indusoft.com/81.2.0/IWS81.2.0.zip
InTouch Edge HMI (formerly InTouch Machine Edition) prior to 2017 SP2	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5223

Vulnerability Characterization and CVSSv3 Rating

CWE-121: Stack-based Buffer Overflow, CWE-258: Empty Password in Configuration

- InduSoft Web Studio and InTouch Edge HMI (formerly InTouch Machine Edition):

  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 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