Date: 11/09/2017

Security Bulletin LFSEC00000124

Title

InduSoft Web Studio and InTouch Machine Edition – Remote Code Execution Vulnerability

Rating

Critical

Published By

Schneider Electric Software Security Response Center

Overview

Schneider Electric Software, LLC ("Schneider Electric") has created a security update to address vulnerabilities in:

- **InduSoft Web Studio v8.0 SP2 Patch 1 and prior versions**
- **InTouch Machine Edition v8.0 SP2 Patch 1 and prior versions**

The vulnerabilities, if exploited, could allow an un-authenticated malicious entity to remotely execute code with high privileges.

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

Recommendations

Customers using **InduSoft Web Studio v8.0 SP2 Patch 1 or prior versions** are affected and should upgrade and apply **InduSoft Web Studio v8.1** as soon as possible.

Customers using **InTouch Machine Edition v8.0 SP2 Patch 1 or prior versions** are affected and should upgrade and apply **InTouch Machine Edition 2017 v8.1** as soon as possible.

Background

InduSoft Web Studio is a powerful collection of tools that provide all the automation building blocks to develop HMIs, SCADA systems and embedded instrumentation solutions. InTouch Machine Edition is a highly scalable, flexible HMI designed to provide everything from advanced HMI applications to small-footprint embedded devices. InduSoft Web Studio and InTouch Machine Edition are used in many industries worldwide, including Manufacturing, Oil and Gas, Water and Wastewater, Building Automation, Automotive, Wind and Solar Power.

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

- On a Windows Desktop or Server operating system, navigate to Windows Programs and Features, locate the "InduSoft Web Studio" or "InTouch Machine Edition" entries and observe 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.

Vulnerability Details

InduSoft Web Studio and InTouch Machine Edition provide the capability for an HMI client to subscribe to tags and monitor their values. A remote malicious entity could send a carefully crafted packet to exploit a stack-based buffer overflow vulnerability during tag subscription, with potential for code to be executed. The code would be executed under high privileges and could lead to a complete compromise of the InduSoft Web Studio or InTouch Machine Edition server machine.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin.
Nov 9, 2017: InduSoft Web Studio v8.1
Nov 9, 2017: InTouch Machine Edition v8.1

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:

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
InduSoft Web Studio v8.0 SP2 Patch 1 or prior	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	http://download.indusoft.com/81.0.0/IWS81.0.0.zip
InTouch Machine Edition v8.0 SP2 Patch 1 or prior	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	https://gcsresource.invensys.com/tracking/ConfirmDownload.aspx?id=22486

Vulnerability Characterization and CVSSv3 Rating

CWE-121: Stack-based Buffer Overflow

- InduSoft Web Studio and ITME: **9.8 |** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Acknowledgements

Schneider Electric would like to thank:
- **Aaron Portnoy formerly of Exodus Intelligence** for the discovery and responsible disclosure of this vulnerability.
- **ICS-Cert** for coordination and advisories.

Support

For information on how to reach Schneider Electric support for your product, please refer to this link: Schneider Electric Software Global Customer Support.

If you discover errors or omissions in this Security Notification, please report the finding to Support.

Wonderware 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