



InduSoft and InTouch Machine Edition Security Bulletin LFSEC00000121

Title

InduSoft Web Studio and InTouch Machine Edition – Remote Arbitrary Command 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 and prior**
- **InTouch Machine Edition v8.0 SP2 and prior**

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

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

This security bulletin announces the software security updates for

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

Recommendations

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

Customers using **InTouch Machine Edition v8.0 SP2 or prior** are affected and should upgrade and apply **InTouch Machine Edition v8.0 SP2 Patch 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 the version of InduSoft Web Studio you have installed, navigate to Windows Programs and Features, locate “InduSoft Web Studio” installation and check the installed version.



Vulnerability Details

InduSoft Web Studio and InTouch Machine Edition provide the capability for an HMI client to trigger script execution on the server for the purposes of performing customized calculations or actions. A remote malicious entity could bypass the server authentication and trigger an arbitrary command to be executed. The command is executed under high privileges and could lead to a complete compromise of the server machine.

Security Update

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

Sept 15, 2017: InduSoft Web Studio v8.0 SP2 Patch 1

Sept 15, 2017: InTouch Machine Edition v8.0 SP2 Patch 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 or prior	Multiple	Confidentiality, Integrity, Availability	Critical	InduSoft Web Studio v8.0 SP2 Patch 1
InTouch Machine Edition v8.0 SP2 or prior	Multiple, Embedded	Confidentiality, Integrity, Availability	Critical	InTouch Machine Edition v8.0 SP2 Patch 1

Vulnerability Characterization and CVSSv3 Rating

[CWE-306](#): Missing Authentication for Critical Function

- 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

THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC AND ITS AFFILIATES, PARENT AND SUBSIDIARIES (COLLECTIVELY, "SCHNEIDER ELECTRIC") DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SCHNEIDER ELECTRIC, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

SCHNEIDER ELECTRIC DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER'S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN SCHNEIDER ELECTRIC'S DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

IN NO EVENT WILL SCHNEIDER ELECTRIC OR ITS SUPPLIERS, DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC'S LIABILITY FOR DAMAGES AND EXPENSES HEREUNDER OR RELATING HERETO (WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE) WILL IN NO EVENT EXCEED THE AMOUNT OF ONE HUNDRED DOLLARS (\$100 USD).