

Schneider Electric Security Notification

EcoStruxure Foxboro SCADA FoxRTU Station

9 July 2024

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Foxboro SCADA FoxRTU Station product.

FoxRTU Station software facilitates configuration, diagnostics, logic development and device management for the SCD2200. The [EcoStruxure™ Foxboro SCADA SCD2200](#) product is a modular Remote Terminal Unit (RTU) for remote SCADA applications.

Failure to apply the remediations provided below may risk remote code execution, which could result in denial-of-service or unauthorized access to system functions.

Affected Products and Versions

Product	Version
FoxRTU Station	All versions prior to v9.3.0

Vulnerability Details

CVE ID: **CVE-2024-2602**

CVSS v3.1 Base Score 7.3 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could result in remote code execution when an authenticated user executes a saved project file that has been tampered by a malicious actor.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 ([CVSS v3.1](#)) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
FoxRTU Station <i>All versions prior to v9.3.0</i>	<p>Version 9.3.0 of FoxRTU Station includes a fix for this vulnerability.</p> <p>Please contact your local Service Representative or Schneider Electric Process Automation Global Customer Support Center for information on how to download and install this fix:</p> <p>Process Automation Global Customer Support (se.com)</p> <p>Please follow the instructions in Chapter 12 of User Guide B0780AE rev. P, “Security: Securing a Project” to encrypt and password protect project files.</p>

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric’s [Customer Care Center](#) if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	Mitigations
FoxRTU Station <i>All versions prior to v9.3.0</i>	<ul style="list-style-type: none"> As the identified vulnerability requires file write access on the machine on which FoxRTU Station is installed, proper file system access control restrictions should be implemented to prevent unauthorized users from editing FoxRTU Station project files or placing malicious DLLs in accessible directories. Store the project files in a secure storage and restrict the access to only trusted users When exchanging files over the network, use secure communication protocols Encrypt project files when stored Only open project files received from trusted source Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices available here:

Schneider Electric Security Notification

	<p>https://www.se.com/us/en/download/document/7EN52-0390/</p> <ul style="list-style-type: none"> To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric’s security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp
--	---

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric [Recommended Cybersecurity Best Practices](#) document.

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2024-2602	Anooja Joy, Sushant Mane and Dr. Faruk Kazi from CoE-CNDS Lab, VJTI, Mumbai, India

Schneider Electric Security Notification

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: <https://www.se.com/ww/en/work/solutions/cybersecurity/>. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

Schneider's purpose is to **create Impact** by empowering all to **make the most of our energy and resources**, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be the trusted partner in **Sustainability and Efficiency**.

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers**.

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

Schneider Electric Security Notification

www.se.com

Revision Control:

Version 1.0.0 <i>09 July 2024</i>	Original Release
---	------------------