

Schneider Electric Security Notification

Deserialization of Untrusted Data vulnerability on EcoStruxure™ Foxboro DCS

10 March 2026 (13 March 2026)

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Foxboro DCS Control Software on Foxboro DCS workstations and servers. Control Core Services and all runtime software, like FCPs, FDCs, and FBMs, are not affected.

The [EcoStruxure™ Foxboro DCS](#) product is an innovative family of fault-tolerant, highly available control components, which consolidates critical information and elevates staff capabilities to ensure flawless, continuous plant operation.

Failure to apply the remediation provided below may risk deserialization of untrusted data, which could result in loss of confidentiality, integrity and potential remote code execution on the compromised workstation.

March 2026 Update: Updated remediation and mitigations section.

Affected Products and Versions

Product	Version
EcoStruxure™ Foxboro DCS	Versions prior to CS8.1

Vulnerability Details

CVE ID: **CVE-2026-1286**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 7.0 | High | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-502: Deserialization of untrusted data vulnerability exists that could lead to loss of confidentiality, integrity and potential remote code execution on workstation when an admin authenticated user opens a malicious project file.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 ([CVSS v4.0](#)). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated 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
EcoStruxure™ Foxboro DCS <i>Versions prior to CS8.1</i>	<p>Version CS 8.1 of EcoStruxure™ Foxboro DCS includes a fix for this vulnerability and is available through https://buyautomation.se.com/</p> <p>CS 8.1 requires FX-V3 licenses, standard upgrade procedures apply. A reboot is required for workstations and servers. Depending on the existing system version, online upgrade without production interruption might be possible.</p> <p>We recommend you work with your local Field Service Representative or Technical Service Consultant for further information.</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
EcoStruxure™ Foxboro DCS <i>Versions prior to CS8.1</i>	<p>The vulnerability is attacked with manipulated data from external sources to the DCS computers. Examples for these are:</p> <ul style="list-style-type: none">• Configuration taglists• DirectAccess Scripts• Any partial or full Galaxy backups• Library files• Code snippets• ASCII files of any sort• Generally, any file getting from outside the DCS computer on a DCS computer. <p>Only using data from trusted sources, check for correct file name endings on data files, check for reasonable file sizes for any files coming to the system, and check structured data for any fields or columns which might be unexpected.</p> <p>Check for unusual manipulations of data within data files and reject files containing unexpected data or structures.</p>

Schneider Electric Security Notification

Use secure communication channels and encrypt communications when communicating outside the site network.

Avoid and ban removable media (e.g. USB sticks or drives)

Minimize count of users with engineering or administrative rights to DCS computers and ensure all interactions on DCS computers are executed with minimal user access rights.

Consequently, isolating Foxboro DCS computers will help minimize the risk of this vulnerability being exploited.

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/notification-contact.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 researcher for identifying and helping to coordinate a response to this vulnerability:

Schneider Electric Security Notification

CVE	Researcher
CVE-2026-1286	Internal Schneider Electric

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 10 March 2026	Original Release
Version 2.0.0 13 March 2026	Updated remediation and mitigations section.