Schneider Electric Security Notification

EcoStruxure™ OPC UA Server Expert and EcoStruxure™ Modicon Communication Server

14 October 2025

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ OPC UA Server Expert product.

The EcoStruxure™ OPC UA Server Expert product is a state-of-the-art OPC UA communication platform linking Modicon industrial equipment and PLCs to the Industrial Internet of Things (IIoT).

EcoStruxure™ Modicon Communication Server is a communication platform seamlessly linking Modicon PLCs to Aveva System Platform by using the OPC UA protocol with the help of OPC UA Server.

Failure to apply the fix / mitigation provided below may risk denial of service of EcoStruxure™ OPCUA Server Expert, which could result in the loss of real-time process data from Modicon Controller.

Affected Products and Versions

Product	Version
EcoStruxure™ OPC UA Server Expert	Versions prior to SV2.01 SP3
EcoStruxure™ Modicon Communication Server	All versions

Vulnerability Details

CVE ID: **CVE-2024-10085**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score 8.2 | High | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-770: Allocation of Resources Without Limits or Throttling vulnerability exists that could cause denial of service of the OPC UA communication platform when a large number of OPC UA requests are sent to the platform.

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.

Remediations

Affected Product & Version	Remediations
EcoStruxure™ OPC UA Server Expert *Versions prior to SV2.01 SP3*	Version SV2.01 SP3 of EcoStruxure™ OPC UA Server Expert includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/66388-ecostruxure-opc-ua-server-expert/#software-and-firmware

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™ OPC UA Server Expert *Versions prior to SV2.01 SP3*	• Set the "Security Policy" to Basic256-Sha256 (default value indicated by unchecked "Security Policy" setting) used for secure communication between OPC UA client & server based on OPC UA standard. • Ensure that the "Anonymous user token" setting remains unchecked (unchecked by default) to prevent anonymous authentication. • Set "User authentication" setting (checked by default) used to authenticate & authorize OPC UA client. • Set "X509 user token" setting (checked by default) used to authenticate & authorize OPC UA client. For more details, refer to "EcoStruxure™ OPC UA Server Expert User Guide" chapter "Security Management": https://www.se.com/ww/en/download/document/MFR53158/ • Follow workstation, network and site-hardening guidelines in the "Recommended Cybersecurity Best Practices": https://www.se.com/ww/en/download/document/7EN52-0390/

EcoStruxure™ Modicon Communication Server *All versions*	Schneider Electric is establishing a remediation plan for all future versions of EcoStruxure™ Modicon Communication Server that will include a fix for this vulnerability. We will update this document when remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Set the "Security Policy" to Basic256-Sha256 (default value indicated by unchecked "Security Policy" setting) used for secure communication between OPC UA client & server based on OPC UA standard. • Ensure that the "Anonymous user token" setting remains unchecked (unchecked by default) to prevent anonymous authentication. • Set "User authentication" setting (checked by default) used to authenticate & authorize OPC UA client. • Set "X509 user token" setting (checked by default) used to authenticate & authorize OPC UA client. For more details, refer to "EcoStruxure™ Modicon Server User Guide" chapter "Security Settings": https://www.se.com/fr/fr/download/document/EIO0000004083/ • Follow workstation, network and site-hardening guidelines in the "Recommended Cybersecurity Best Practices": https://www.se.com/ww/en/download/document/7EN52-0390/

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 researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2024-10085	Jin Huang (ADLab of Venustech)

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.

Schneider Electric Security Notification

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**.

www.se.com

Revision Control:

Version 1.0.0 *14 October 2025*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2025.10.13 21:50:36 -04'00'