Schneider Electric Security Notification

EcoStruxure™ OPC UA Server Expert

11 July 2023

Overview

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

EcoStruxure™ OPC UA Server Expert is a communications platform seamlessly linking Schneider Electric PLCs and connected devices to enterprise information systems and the Industrial Internet of Things (IIoT) via the OPC Foundation's Open Platform Communications – Unified Architecture (OPC UA) service-oriented architecture standard.

Failure to apply the remediation provided below may risk confidentiality, which could result in disclosure of sensitive information from the system running the software.

Affected Products and Versions

Product	Version
EcoStruxure™ OPC UA Server Expert	Versions prior to SV2.01 SP2

Vulnerability Details

CVE ID: **CVE-2023-37200**

CVSS v3.1 Base Score 5.5 | Medium | AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

A *CWE-611: Improper Restriction of XML External Entity Reference* vulnerability exists that could cause loss of confidentiality when replacing a project file on the local filesystem and after manual restart of the server.

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
EcoStruxure™ OPC UA Server Expert Versions prior to SV2.01 SP2	Version SV2.01 SP2 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:

- Follow workstation, network, and site-hardening guidelines in the Recommended Cybersecurity Best Practices Guide available for download here.
- Only open project configuration files received from a trusted source.
- Encrypt project configuration files when stored and restrict access to only trusted users.
- When exchanging files over network, use secure communication protocols.

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-2023-37200	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

Schneider Electric Security Notification

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 empower 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 your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *11 July 2023*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2023.07.10 08:31:30 -04'00'