

Schneider Electric Security Notification

EcoStruxure™ Control Expert

11 April 2023 (09 January 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities in its [EcoStruxure™ Control Expert](#) product.

[EcoStruxure™ Control Expert](#) is the common programming, debugging and operating software for Modicon PLCs (Programmable Logic Controllers) and PACs (Programmable Automation Controllers).

Failure to apply the remediations provided below may risk arbitrary code execution & privilege escalation which could result in denial of service, loss of confidentiality and integrity of the software

January 2024 Update: A remediation is available for EcoStruxure™ Control Expert.

Affected Products and Versions

Product	Versions
EcoStruxure™ Control Expert	Versions prior to v16.0

Vulnerability Details

CVE ID: **CVE-2023-27976**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-668: Exposure of Resource to Wrong Sphere* vulnerability exists that could cause remote code execution when a valid user visits a malicious link provided through the web endpoints.

CVE ID: **CVE-2023-1548**

CVSS v3.1 Base Score 5.5 | Medium | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A *CWE-269: Improper Privilege Management* vulnerability exists that could cause a local user to perform a denial of service through the console server service that is part of EcoStruxure™ Control Expert.

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

Schneider Electric Security Notification

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.

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Control Expert <i>Versions prior to v16.0</i>	Version 16.0 of EcoStruxure Control Expert includes fixes for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/548-ecostruxure-control-expert-unity-pro/#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™ Control Expert <i>Versions prior to v16.0</i>	<ul style="list-style-type: none"> EcoStruxure™ Control Expert v15.3 mitigates the CVE-2023-27976 by restricting the remote exploitation of this vulnerability. It is available for download below: https://www.se.com/ww/en/download/document/EcoStruxureControlExpert-V15.3/ Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices guide available for download here. To help protect workstations running Schneider Electric and other user applications against execution of unauthorized applications and malicious files, Schneider Electric recommends using McAfee Application and Change Control software. Refer to the Cybersecurity Application Note available here.

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>

Schneider Electric Security Notification

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 these vulnerabilities:

CVE	Researcher
CVE-2023-1548 CVE-2023-27976	Ruben Santamarta

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.

Schneider Electric Security Notification

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 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 1.0.0 <i>11 April 2023</i>	Original Release
Version 2.0.0 <i>09 January 2024</i>	A remediation is now available for EcoStruxure™ Control Expert.