Schneider Electric Security Notification

EcoStruxure™ Cybersecurity Admin Expert

14 June 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Cybersecurity Admin Expert product.

The EcoStruxure™ Cybersecurity Admin Expert (CAE) product is a solution for managing cybersecurity in an electrical network's operational technology (OT).

Failure to apply the remediation provided below may risk man-in-the-middle and/or device spoofing attacks, which could result in the total compromise of devices configured by the CAE.

Affected Product and Version

Product	Version
EcoStruxure™ Cybersecurity Admin Expert (CAE)	Versions 2.2 and prior

Vulnerability Details

CVE ID: **CVE-2022-32747**

CVSS v3.1 Base Score 8.0 | High | CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-290: Authentication Bypass by Spoofing* vulnerability exists that could cause legitimate users to be locked out of devices or facilitate backdoor account creation by spoofing a device on the local network.

CVE ID: **CVE-2022-32748**

CVSS v3.1 Base Score 7.9 | High | CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

A *CWE-295: Improper Certificate Validation* vulnerability exists that could cause the CAE software to give wrong data to end users when using CAE to configure devices. Additionally, credentials could leak which would enable an attacker the ability to log into the configuration tool and compromise other devices in the network.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Cybersecurity Admin Expert (CAE) *Versions 2.2 and prior*	Version 2.4 of the EcoStruxure™ Cybersecurity Admin Expert product includes fixes for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/63515-ecostruxure-cybersecurity-admin-expert/#software-and-firmware Install the new CAE version 2.4 (over any previous version) and the fixes will be available.

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:

In normal operation, the CAE software tool is connected to devices for a very limited time and is offline most of the time. However, it is recommended that end-users of the Cybersecurity Admin Expert tool do the following:

- Refresh the device's status before sending configuration to ensure the validity of the devices certificate.
- Use proper network segmentation and closely monitor traffic for signs of malicious activity when connected to devices
- Check the status of the devices on the network

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-2022-32747, CVE-2022-32748	U.S. Department of Energy CyTRICS researcher McKade Umbenhower –INL

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

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 *14 June 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.06.13 11:36:07 -04'00'