Schneider Electric Security Notification

EcoStruxure™ Power SCADA Anywhere

10 January 2023

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Power SCADA Anywhere product.

EcoStruxure™ Power SCADA Anywhere is an on-premises software that provides remote web browser access to the EcoStruxure Power Operation desktop HMI client application and its operator interface.

Failure to apply with the mitigations provided below may risk an authenticated user to escape from the context of EcoStruxure™ Power SCADA Anywhere into the Operating System (OS), which could result in arbitrary OS commands being executed on the system.

Affected Products and Versions

Product	Version
EcoStruxure™ Power SCADA Anywhere	2022, 2021, 2020 R2, 2020, 9.0, 8.x

Vulnerability Details

CVE ID: **CVE-2022-1467**

CVSS v3.1 Base Score 7.4 | High | AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

A *CWE-668: Exposure of Resource to Wrong Sphere* vulnerability exists that could cause an authenticated user to run arbitrary OS commands at restricted privileged levels if exploited.

Schneider Electric Security Notification

Mitigations

Affected Product & Version	Mitigations
EcoStruxure™ Power SCADA Anywhere *Version: 2022, 2021, 2020 R2, 2020, 9.0, 8.x*	Windows OS can be configured to overlay a "Language Bar" on top of any application. When this OS functionality is enabled, the OS Language Bar UI will be viewable in the browser alongside EcoStruxure™ Power SCADA Anywhere. It is possible to abuse the Windows OS Language Bar to launch an OS Command Prompt, resulting in a context-escape from application into OS. Schneider Electric recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation. If impacted, we recommend customers consider applying the following mitigations to reduce the risk of exploit: • Disable the Windows Language Bar on the server machine hosting EcoStruxure™ Power SCADA Anywhere, unless it is required for corporate policy. • Create unique user accounts with minimal privileges dedicated only to remote access of the EcoStruxure™ Power SCADA Anywhere application. • Utilize OS Group Policy Objects (GPO) to further restrict what those unique user accounts are allowed to do. • Restrict access based on Microsoft's recommended block list: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules 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/ww/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.

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

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 *10 January 2023*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2023.01.09 12:40:47 -05'00'