Schneider Electric Security Notification

EcoStruxure™ Power Operation

EcoStruxure™ Power SCADA Operation

9 May 2023

Overview

Schneider Electric is aware of multiple vulnerabilities in the AVEVA™ Plant SCADA product which is included as part of EcoStruxure™ Power Operation, EcoStruxure™ Power SCADA Operation products.

EcoStruxure™ Power Operation and EcoStruxure™ Power SCADA Operation are on-premises software offers that provides a single platform to monitor and control medium and lower power systems.

Failure to apply the remediations or mitigations provided below may risk escalation of privileges, which could result in an unauthenticated user being able to remotely read data, cause denial of service, and tamper with alarm states.

Details

A critical vulnerability disclosed by AVEVA in Plant SCADA impacts Schneider Electric EcoStruxure™ Power Operation and EcoStruxure™ Power SCADA Operation products.

Additional information about the vulnerability can be found in the AVEVA Security Bulletin at AVEVA-2023-002.

Affected Products and Versions

Product	Version
EcoStruxure™ Power Operation	Version 2022 Versions 2021 CU3 and prior
EcoStruxure™ Power SCADA Operation	Versions 2020 R2 and prior

Schneider Electric Security Notification

Remediation & Mitigations

Affected Product & Version	Remediation
EcoStruxure™ Power Operation *Version 2022*	EcoStruxure™ Power Operation 2022 CU1 includes a fix for this vulnerability and is available for download here: https://community.se.com/t5/EcoStruxure-Power-Operation/v2022-Release-amp-Updates-Install-Procedure/m-p/416561/thread-id/6058 Please note: these updates are made available through the Schneider Electric Exchange community. If you are unable to access this service, please contact Schneider Electric Customer Care Center for assistance in accessing these updates.
EcoStruxure™ Power Operation *Versions 2021 CU3 and prior*	EcoStruxure™ Power Operation 2021 version CU3 and prior is available here: https://community.se.com/t5/EcoStruxure-Power-Operation/v2021-Release-amp-Updates-Install-Procedure/td-p/358628 *Requires EPO 2021 CU3 to be installed prior to applying this Plant SCADA update. Please note: these updates are made available through the Schneider Electric Exchange community. If you are unable to access this service, please contact Schneider Electric Customer Care Center for assistance in accessing these updates.
EcoStruxure™ Power SCADA Operation *Versions 2020 R2 and prior*	These products are no longer supported. Please contact the Customer Care Center for upgrade options. Additionally ensure that the Recommended Cybersecurity Best Practices are implemented to reduce exploitability. 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

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.

Schneider Electric Security Notification

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit.

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 *09 May 2023*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2023.05.08 12:41:41 -04'00'