Schneider Electric Security Notification

Power SCADA Anywhere

9 May 2023

Overview

Schneider Electric is aware of multiple vulnerabilities in the AVEVA™ Plant SCADA Access Anywhere which is an optional component of the EcoStruxure™ Power Operation or EcoStruxure™ Power SCADA Operation products.

EcoStruxure™ Power SCADA Anywhere is a web based remote access tool.

Details

Three vulnerabilities disclosed by AVEVA in the Plant SCADA Access Anywhere product may impact customers who have installed the Power SCADA Anywhere optional component of Schneider Electric's EcoStruxure™ Power Operation or EcoStruxure™ Power SCADA Operation products.

Additional information about the vulnerabilities can be found in the AVEVA Security Bulletin at [AVEVA-2023-001](#).

Note: As the vulnerabilities lie in an optional component, customers who have installed EcoStruxure™ Power Operation or EcoStruxure™ Power SCADA Operation without Power SCADA Anywhere are not impacted by these vulnerabilities.

Affected Products and Versions

Product	Version
EcoStruxure™ Power Operation or EcoStruxure™ Power SCADA Operation configured with Power SCADA Anywhere	Power SCADA Anywhere Versions 1.1 and 1.2

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Power Operation or **EcoStruxure™ Power SCADA Operation** configured with Power SCADA Anywhere versions 1.1 or 1.2	Version 2023 of Plant SCADA Anywhere (formerly known as Power SCADA Anywhere) includes a fix for these vulnerabilities and is available for download here: https://community.se.com/t5/EcoStruxure-Power-Operation/Power-SCADA-Anywhere/m-p/147702 Please note: This update is 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.

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

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN

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