Schneider Electric Security Notification

EcoStruxure™ Machine SCADA Expert / BLUE Open Studio

13 August 2024

Overview

Schneider Electric is aware of a vulnerability disclosed on AVEVA component used in EcoStruxure™ Machine SCADA Expert and BLUE Open Studio products.

The EcoStruxure™ Machine SCADA Expert is software for developing HMI, SCADA, OEE and Dashboard projects dedicated to Line Management & Lite Supervision applications to run in Harmony Industrial PC and GTU Open Box.

Pro-face BLUE Open Studio is a development and runtime software that incorporates tools users need to create SCADA HMI applications, dashboards, and OEE interfaces.

Failure to apply the remediation provided below may risk privilege escalation and/or Arbitrary code execution which could result in information disclosure, integrity loss or denial of service.

Affected Products and Versions

Product	Version
EcoStruxure™ Machine SCADA Expert	Version prior to 2020 SP3 HF1
Pro-face BLUE Open Studio	Version prior to 2020 SP3 HF1

Vulnerability Details

Vulnerability disclosed by AVEVA Group Limited in its component impacts Schneider Electric software. Additional information about the vulnerabilities can be found in the AVEVA Advisories at:

AVEVA Security Advisory (AVEVA -2024-002)

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
EcoStruxure Machine SCADA Expert *Versions prior to 2020 SP3 HF1*	Version 2023 release or later of EcoStruxure™ Machine SCADA Expert includes a fix for this vulnerability and is available for download https://www.se.com/ww/en/product-range/63734-ecostruxure-machine-scada-expert/#software-and-firmware. Version 2020 SP3 HF1 release of EcoStruxure™ Machine SCADA Expert includes a fix for this vulnerability. Please contact your Schneider Electric Customer Care Center to obtain the Hot Fix. For additional details please refer to the supplied help file in Hot Fix 2020 SP3 HF1.
BLUE Open Studio *Versions prior to 2020 SP3 HF1*	Version 2023 release or later of BLUE Open Studio includes a fix for this vulnerability and is available for download https://www.proface.com/en/news/2023/1117_1. Version 2020 SP3 HF1 release of BLUE Open Studio includes a fix for this vulnerability. Please contact your Pro-face Customer Care Center to obtain the Hot Fix. For additional details please refer to the supplied help file in Hot Fix 2020 SP3 HF1.

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:

- Access Control Lists should be applied to all folders where users will save and load project files.
- Maintain a trusted chain-of-custody on project files during creation, modification, distribution, and use.
- Train users to always verify the source of a project is trusted before opening or executing it.

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.

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

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 **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency.**

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers.**

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 *13 August 2024*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.08.12 12:14:10 -04'00'