Schneider Electric Security Notification

EcoStruxure Machine SCADA Expert and Pro-face BLUE Open Studio

13 September 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure Machine SCADA Expert and Pro-face BLUE Open Studio products.

EcoStruxure Machine SCADA Expert is a powerful 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 all of the tools users need to create SCADA HMI applications, dashboards and OEE interfaces.

Failure to apply the mitigations provided below may risk a modification of project files which could result in arbitrary code execution, information disclosure, or denial of service.

Affected Products and Versions

Product	Version
EcoStruxure Machine SCADA Expert 2020 Service Pack 2	V20.0.2 or prior
BLUE Open Studio 2020 Service Pack 2	V20.0.2 or prior

Vulnerability information

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE-502: *Deserialization of Untrusted Data* vulnerability exists that can lead to arbitrary code execution, information disclosure, or denial of services when the project file is loaded. Successful exploitation of the vulnerability requires user interaction and write access to HMI project file.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
EcoStruxure Machine SCADA Expert 2020 Service Pack 2 *V20.0.2 or prior*	Version 2020 Service Pack 2 Hot Fix 2020.2.00.40 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 detail please refer to the supplied help file in Hot Fix 2020.2.00.40.
BLUE Open Studio 2020 Service Pack 2 *V20.0.2 or prior*	Version 2020 Service Pack 2 Hot Fix 2020.2.00.40 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 detail please refer to the supplied help file in Hot Fix 2020.2.00.40.

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:

- Install physical controls so no unauthorized personnel can access your HMI Device, Laptop, and engineering workstation.
- Harden your network and engineering workstation following the best cybersecurity practices (antivirus, updated operating systems, strong password policies, application allow list software, etc.) using the Recommended Cybersecurity Best Practices document.

In addition to applying the remediations provided above, the following general precautions should be taken throughout the lifetime of EcoStruxure Machine SCADA Expert projects and BLUE Open Studio projects:

- Access Control Lists should be applied to all folders where users will save and load project files.
- Enforce a trusted chain-of-custody on project files, maintained during creation, modification, distribution, and use.

- Train users to always verify the source of a project is trusted before opening/executing it.

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

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 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 *13 September 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.09.09 15:57:22 -04'00'