Schneider Electric Security Notification

EcoStruxure™ Operator Terminal Expert and Pro-face BLUE

11 October 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Operator Terminal Expert and Pro-face BLUE products.

The EcoStruxure™ Operator Terminal Expert and Pro-face BLUE products are HMI configuration software supporting gestures and UI designs.

Failure to apply the remediations provided below may risk unauthorized code execution by a local user of the Windows engineering workstation, which could result in loss of availability, integrity, and confidentiality of the workstation where EcoStruxure™ Operator Terminal Expert or Pro-face BLUE runtime is installed.

Affected Products and Versions

Product	Version
EcoStruxure™ Operator Terminal Expert	V3.3 Hotfix 1 or prior
Pro-face BLUE	V3.3 Hotfix1 or prior

Vulnerability Details

CVE ID: **CVE-2022-41666**

CVSS v3.1 Base Score 7.0 | High | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-347: Improper Verification of Cryptographic Signature* vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code.

CVE ID: **CVE-2022-41667**

CVSS v3.1 Base Score 7.0 | High | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that allows adversaries with local user privileges to load a malicious DLL which could lead to execution of malicious code.

CVE ID: **CVE-2022-41668**

CVSS v3.1 Base Score 7.0 | High | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-704: Incorrect Project Conversion* vulnerability exists that allows adversaries with local user privileges to load a project file from an adversary-controlled network share which could result in execution of malicious code.

Schneider Electric Security Notification

CVE ID: **CVE-2022-41669**

CVSS v3.1 Base Score 7.0 | High | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-347: Improper Verification of Cryptographic Signature* vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load a malicious DLL which could result in execution of malicious code.

CVE ID: **CVE-2022-41670**

CVSS v3.1 Base Score 7.0 | High | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists in the SGIUtility component that allows adversaries with local user privileges to load malicious DLL which could result in execution of malicious code.

CVE ID: **CVE-2022-41671**

CVSS v3.1 Base Score 7.0 | High | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-89: Improper Neutralization of Special Elements used in SQL Command ('SQL Injection')* vulnerability exists that allows adversaries with local user privileges to craft a malicious SQL query and execute as part of project migration which could result in execution of malicious code.

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Operator Terminal Expert *V3.3 Hotfix 1 or prior*	EcoStruxure™ Operator Terminal Expert V3.3 Service Pack 1 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/62621-ecostruxure-operator-terminal-expert/#software-and-firmware This fix is also available through Schneider Electric Software Update (SESU).
Pro-face BLUE *V3.3 Hotfix1 or prior*	Pro-face BLUE V3.3 Service Pack 1 includes a fix for these vulnerabilities and is available for download here: https://www.proface.com/en/service#/blue/page/installer This fix is also available through Schneider Electric Software Update (SESU).

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 or Pro-face'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:

- Use EcoStruxure™ Operator Terminal Expert and Pro-face BLUE software in a secure network environment.
- Use EcoStruxure™ Operator Terminal Expert and Pro-face BLUE software only on a trusted workstation.
- Harden your workstation following the best cybersecurity practices (antivirus, updated operating systems, strong password policies, application whitelisting software, etc.) using the Schneider Electric Recommended Cybersecurity Best Practices document.

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.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2022-41666 CVE-2022-41667 CVE-2022-41668 CVE-2022-41669 CVE-2022-41670 CVE-2022-41671	Noam Moshe and Amir Preminger (Claroty)

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

About Schneider Electric

Schneider Electric Security Notification

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 *11 October 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.10.10 13:19:42 -04'00'