Schneider Electric Security Notification

EcoStruxure™ Operator Terminal Expert and Pro-face BLUE

12 January 2021

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Operator Terminal Expert (formerly known as Vijeo XD) 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 remediation instructions provided below may risk arbitrary code execution, which could result in loss of availability, confidentiality, and integrity of the HMI where EcoStruxure™ Operator Terminal Expert / Pro-face BLUE is running.

Affected Products and Versions

EcoStruxure™ Operator Terminal Expert 3.1 Service Pack 1A and prior running on Harmony HMIs:

- HMIST6 Series
- HMIG3U in HMIGTU Series
- HMISTO Series

Pro-face BLUE 3.1 Service Pack 1A and prior running on Pro-face HMIs:

- ST6000 Series
- SP-5B41 in SP5000 Series
- GP4100 Series

Vulnerability Details

CVE ID: **CVE-2020-28221**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the Ethernet Download feature is enable on the HMI.

Remediation

- V3.1 Service Pack 1B of the **EcoStruxure™ Operator Terminal Expert** includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range-download/62621-ecostruxure%E2%84%A2-operator-terminal-expert/#/software-firmware-tab
    - This fix is also available through Schneider Electric Software Update (SESU)

- V3.1 Service Pack 1B of **Pro-face BLUE** includes a fix for this vulnerability and is available for download here:

  https://www.proface.com/en/service#/page/installer/blue

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.

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

- Disable the"Always Allow Ethernet Transfer" option in [Target] -[Advanced] -[Settings] - [Preferences] in the project
- Use Harmony and Pro-face HMIs in a secure network environment

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 for the devices that it is intended for.
- 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. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.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 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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *12 January 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.01.08 17:59:25 -05'00'