Schneider Electric Security Notification

EcoStruxure™ Operator Terminal Expert (Vijeo XD), Pro-face BLUE and WinGP runtime (V2.0)

10 November 2020 (12 January 2021)

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Operator Terminal Expert (formerly known as Vijeo XD), Pro-face BLUE and WinGP runtimes. This vulnerability impacts Windows PC and Harmony iPC offers.

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

WinGP is a runtime engine on Windows PC and is included in Pro-face GP-Pro EX product which is an HMI Screen Editor & Logic Programming Software for Pro-face.

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

January 2021 update: Added Pro-face BLUE and WinGP to the list of products affected and links to the fixes

Affected Product and Version

EcoStruxure™ Operator Terminal Expert Runtime 3.1 Service Pack 1A and prior installed on:

- Windows PC using legacy BIOS
- Harmony iPC(HMIG3U) using legacy BIOS

Pro-face BLUE Runtime 3.1 Service Pack 1A and prior installed on:

- Windows PC using legacy BIOS
- Pro-face iPC (SP-5B10) using legacy BIOS

WinGP V4.09.120 and prior installed on:

- Windows PC using legacy BIOS
- Pro-face PS4000 & PS5000 series and SP-5B40, SP5B41 using legacy BIOS

Note : Windows PC using UEFI are not impacted by this vulnerability.

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2020-7544**

CVSS v3.0 Base Score 7.4 | High | CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

A CWE-269 Improper Privilege Management vulnerability exists that could cause privilege escalation on the workstation when interacting directly with a driver installed by the runtime software of EcoStruxure™ Operator Terminal Expert or Pro-face BLUE or WinGP.

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 the **Pro-face BLUE** includes a fix for this vulnerability and is available for download here: https://www.proface.com/en/service#/page/installer/blue

- V4.09.200 of the **WinGP,** included in GP-Pro EX, includes a fix for this vulnerability and is available for download here: https://www.proface.com/en/download/trial/gpproex/v40
    - Reinstall WinGP on the affected products

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:

- Use EcoStruxure™ Operator Terminal Expert, Pro-face BLUE, or WinGP software only on a trusted workstation.
- Harden your workstation following the best cybersecurity practices (antivirus, updated operating systems, strong password policies, application White Listing software, etc.) using the following guideline: https://www.se.com/us/en/download/document/CS-Best-Practices-2019-340/
- Use Windows PC with UEFI technology. Customers can identify if their PC uses the UEFI technology by using the following system command: **msinfo32.exe** provided by Microsoft Windows. This command provides the system information. The section **BIOS mode** displays either "UEFI" or "LEGACY".
    - If the value is UEFI, the PC is not vulnerable, if the value is LEGACY then the PC is vulnerable

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 laptops 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.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher
CVE-2020-7544	Lasse Trolle Borup (Danish Cyber Defence)

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

Schneider Electric Security Notification

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 1.0 *10 November 2020*	Original Release
Version 2.0 *12 January 2021*	Pro-face BLUE and WinGP added to list of affected products (page 1-2)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.01.08 17:24:01 -05'00'