

Schneider Electric Security Notification

Pro-face GP-Pro EX Programming Software

12 May 2020

Overview

Schneider Electric is aware of a vulnerability in the Pro-face GP-Pro EX Programming Software product.

Affected Product(s)

GP-Pro EX V1.00 to V4.09.100

Vulnerability Details

CVE ID: **CVE-2020-7492**

CVSS v3.0 Base Score 5.5 | Medium | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

A CWE-521: Weak Password Requirements vulnerability exists which could cause the discovery of the password when the user is entering the password because it is not masqueraded.

Remediation

This vulnerability is fixed in version GP-Pro EX V4.09.120 and is available for download below:

<https://www.proface.com/en/node/47334>

Product Information

The Pro-face GP-Pro EX Programming Software is an HMI Development Software that supports Dedicated and Open HMI (PC-based) solutions.

Product Category - All Categories

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

Learn more about Pro-Face product categories here: <https://www.proface.com/en/>

Schneider Electric Security Notification

How to determine if you are affected

All users of GP-Pro EX software.

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.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2020-7492	Kirill Kruglov (Kaspersky Lab)

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, please contact your local Schneider Electric representative and/or Schneider Electric Industrial

Schneider Electric Security Notification

Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

<http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page>

<https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. 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 **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 12 May 2020	Original Release
---------------------------------	-------------------------