Schneider Electric Security Notification

Schneider Electric PACTware (V1.1)

11 August 2020 (13 August 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities in the PACTware product.

Affected Product(s)

Schneider Electric PACTware V5.0.5.30 and prior.
Schneider Electric PACTware V4.1 SP5 and prior.

Vulnerability Details

CVE ID: CVE-2020-9403

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

In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in a recoverable format, and may be retrieved by any user with access to the PACTware workstation.

CVE ID: CVE-2020-9404

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H|

In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in an insecure manner, and may be modified by an attacker with no knowledge of the current passwords.

Remediation

This vulnerability is fixed in versions V4.1 SP6a and V5.0.5.31 available for download below:

4.1 SP6a is available through Global Customer Support site as TD70270673 at:

https://pasupport.schneider-electric.com/qfdb/qfdisplay/search/searchresultframe.asp?QuickFixName=HF70270673&chkShowSuperseded=on

V5.0.5.31 is available at:

https://www.se.com/ww/en/download/document/FD-SOFT-M-026/

Schneider Electric Security Notification

Product Information

PACTware is a software application for easy operation of automation field devices.

Product Category - Industrial Automation Control

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

How to determine if you are affected

If you are running PACTware version 5.0.5.30 or earlier or version V4.1 SP5 or earlier. The version information can be found under the Help -> About pull down on upper right side of the PACTware main screen.

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.

Schneider Electric Security Notification

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

https://www.se.com/us/en/work/support/

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

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 *11 August 2020*	Original Release
Version 1.1 *13 August 2020*	Updated version from *V4.1 SP6* to *V4.1 SP6a*

Product Security Office

Digitally signed by Product Security Office
Date: 2020.08.13 16:50:49 -04'00'