PACT*ware* Consortium e.V.

Cyber Security Notification

May 29, 2020

PACT*ware* Document Reference Number

PWC-VD-2020-01

Publication date

2020-05-29

Overview

The software product PACT*ware* is a manufacturer and fieldbus-independent operating software for all field devices and protocols.

PACT*ware* Consortium is aware of a vulnerability in the PACT*ware* Software product.

Affected products

All PACT*ware* versions:

- PACT*ware* 5.0.4.xx and lower
- PACT*ware* 4.1 SP5 and lower
- PACT*ware* 3.X and lower
- PACT*ware* 2.4 and lower

Vulnerabilities Details

CVE Identifier

CVE: Common Vulnerabilities and Exposures

1. CVE-2020-9403
2. CVE-2020-9404

Severity

CVSS: Common Vulnerability Scoring System

1. 5.5 (CVSS: 3 /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
2. 7.1 (CVSS: 3 /AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H)

Vulnerability Type

1. Storing Passwords in a Recoverable Format (CWE-257)
2. Unverified Password Change (CWE-620)

Summary

1. PACT*ware* passwords are stored in a recoverable format
2. PACT*ware* passwords may be modified without knowing the current password

Impact

PACT*ware* supports 'user roles', which limit user access according to FDT Guidelines. By default, no passwords are set and the default user has the user role 'admin' with no limitations.
If the user enables role access control, each role may be protected with an individual password.

These settings could be changed by a local user without any verification. This means a local user may modify role enablement, and role passwords, without authenticating first. (CVE-2020-9404)
The settings can be read by a local user with no verification. It is possible to recover passwords for the roles, if passwords were previously set. (CVE-2020-9403)
If the user has not enabled individual roles, an attacker may enable the roles and assign passwords to them. This could block legitimate users from using the software.

Solution

PACT*ware* will protect the manipulation of stored passwords by using a salted mechanism of password encryption with an additional SHA256 hash. (CVE-2020-9403)
Any further changes in 'user role'-administration will need a confirmation by using the current login password. (CVE-2020-9404)

This will be fixed in following versions (and higher)

- PACT*ware* 5.0.5.31
- PACT*ware* 4.1 SP6

Overview about version history: https://pactware.com/de/service

You can protect yourself against manipulation by restricting the access to the PC where PACT*ware* is installed.

In case of not known passwords it can be reset by
- re-installation of PACT*ware* (all PACT*ware* versions).

Acknowledgements to Researchers and VDE

PACTware Consortium e.V. recognizes

- the researcher Reid Wightman from Dragos, Inc for identifying the security vulnerability and
- Jochen Becker und Andreas Harner from CERT@VDE and Jens Wiesner from BSI for helping to coordinate a response to our users.

Support

For support and service, please contact info@pactware.com or the responsible PACT*ware* member of your distribution.
Downloads of new releases:

- Download-area of your PACT*ware* distributor or
- Otherwise: list of download links from some PACTware members: https://pactware.com/products/pactware

PACT*ware* Consortium e.V.
Business Office
Panoramastr. 16

76327 Pfinztal / Germany

Phone + 49 (0) 7240 94309-61
Fax + 49 (0) 7240 94309-63
Email: info@pactware.com
www.pactware.com