SECURITY BULLETIN 2025-1

LIBRARIES UPDATES IN PCVUE 16.2.5 AND PCVUE 16.3.0

SUMMARY:

This document contains information about major updates of third-party libraries in PcVue 16.2.5 and PcVue 16.3.0.

Reference	SB2025-1
Publication date	2025.04.30
Last update	2025.06.04
Confidentiality	TLP:CLEAR

Date	Revision	Action
2025.04.30	1.0	Initial version
2025.05.15	Rev A	(technical) Updated section “Available patches” (fixed in PcVue 16.2.5)
2025.06.04	Rev B	(technical) Added libraries libpng, qt and zlib, used by the Video control component, that have been updated in PcVue 16.3.0 only

1. Overview

ARC Informatique is aware of potential security vulnerabilities affecting PcVue.

PcVue relies on a number of third-party libraries and dependencies, some of which may present vulnerabilities that could impact the security of our products.

This bulletin lists the vulnerable libraries updated in the Maintenance Release 16.2.5 and in the Feature Release 16.3.0.

2. Affected libraries and components

Library/dependency	Affected components	Affected versions	Description
DotNetZip		PcVue 16.2.4 and earlier versions	Ad'hoc fix based on version 1.6.0. It notably fixes CVE-2024-48510
expat	Add-on ICCP	PcVue 16 PcVue 15.1.0	Updated from version 2.4.0 to 2.6.4 It notably fixes CVE-2023-52425, CVE-2023-52426, CVE-2024-45490, CVE-2024-45491 and CVE-2024-45492
gRPC		PcVue 16.2.4	Updated from version 1.60.0 to 1.68.2 It notably fixes CVE-2024-11407
libpng	Video control	PcVue 16	Updated from version 1.6.20 to 1.6.37 It notably fixes CVE-2016-10087, CVE-2017-12652 and CVE-2019-7317
mbedTLS		PcVue 16.2.4	Updated from version 3.6.1 to 3.6.2 It notably fixes CVE-2024-49195
Mosquitto	Add-on MQTT	PcVue 16 PcVue 15	Updated from version 2.0.18 to 2.0.20 It notably fixes CVE-2024-3935, CVE-2024-8376 and CVE-2024-10525
OpenSSL		PcVue 16 PcVue 15 PcVue 12	Updated from version 3.3.2 to 3.4.1 It notably fixes CVE-2024-9143 and CVE-2024-13176
qt	Video control	PcVue 16	Library no longer used. It fixes multiple vulnerabilities.
zlib	Video control	PcVue 16	Updated from version 1.2.5 to 1.2.13 It notably fixes CVE-2016-9840, CVE-2016-9841, CVE-2016-9842 and CVE-2016-9843

3. Impact

The exact impact on a particular system depends on many factors. According to the vulnerabilities described hereafter, we recommend that each user of the affected products evaluate the risk for their system.

4. Immediate risk mitigation

4.1 Harden the configuration

Who should apply this recommendation: All users
The system operators are highly recommended to take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet unless required.
- Locate control system networks and remote devices behind firewalls and isolate them from business networks.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

4.2 Update PcVue

Who should apply this recommendation: All users using the affected component
Apply the patch by installing a fixed PcVue version.

5. Available patches

Component	Description
DotNetZip	Fixed in: • PcVue 16.2.5 and PcVue16.3.0
expat	Fixed in: • PcVue 16.2.5 and PcVue 16.3.0
gRPC	Fixed in: • PcVue 16.2.5 and PcVue 16.3.0
libpng	Fixed in: • PcVue 16.3.0
mbedTLS	Fixed in: • PcVue 16.2.5 and PcVue 16.3.0
Mosquitto	Fixed in: • PcVue 16.2.5 and PcVue 16.3.0
OpenSSL	Fixed in: • PcVue 16.2.5 and PcVue 16.3.0
qt	Fixed in: • PcVue 16.3.0
zlib	Fixed in: • PcVue 16.3.0

6. Credits

N/A

7. References

The public ARC Informatique security alert page: www.pcvue.com/security

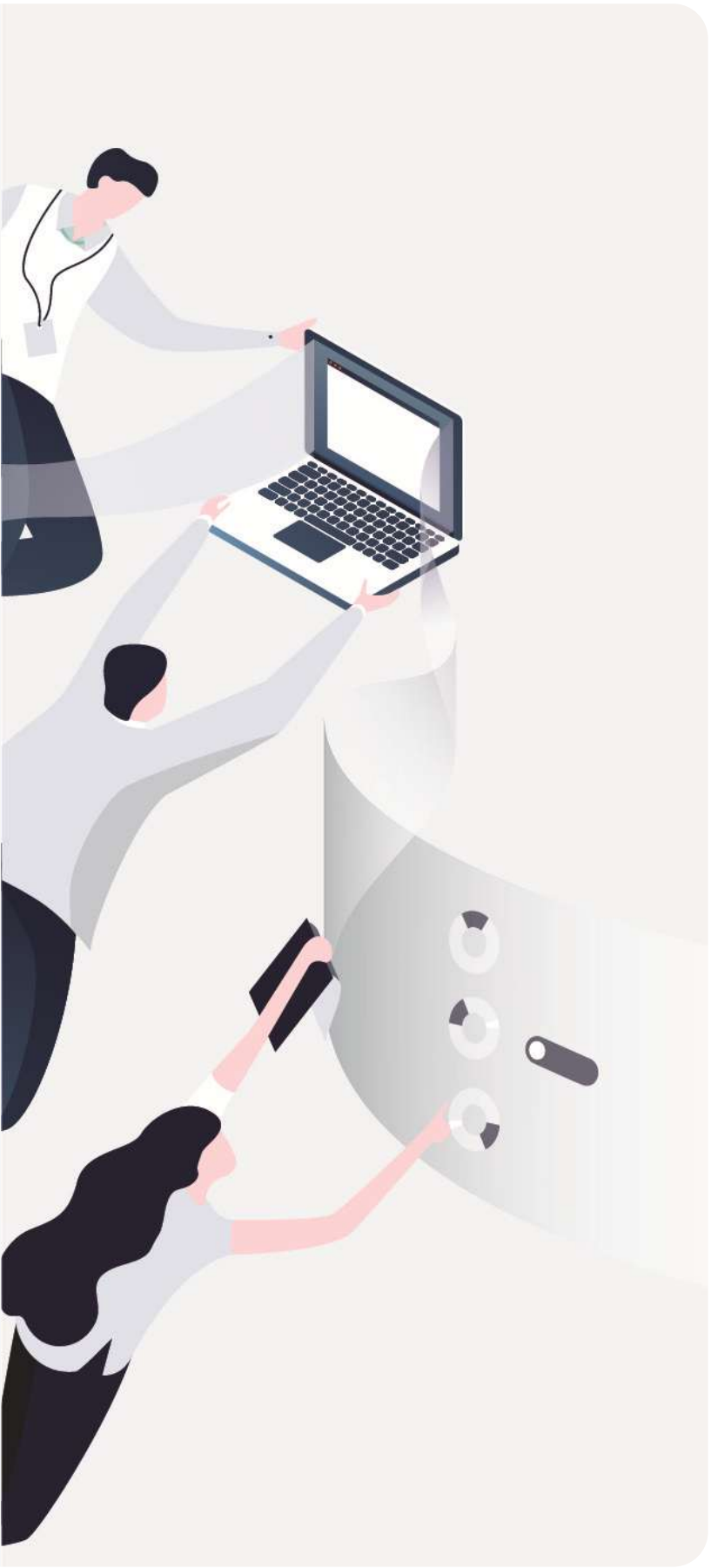
ARC Informatique's SPR Ids: SPR #74587, 74712

CVE:

- Library DotNetZip: CVE-2024-48510
- Library expat: CVE-2023-52425, CVE-2023-52426, CVE-2024-45490, CVE-2024-45491 and CVE-2024-45492
- Library gRPC: CVE-2024-11407
- Library libpng: CVE-2016-10087, CVE-2017-12652 and CVE-2019-7317
- Library mbedTLS: CVE-2024-49195
- Library Mosquitto: CVE-2024-3935, CVE-2024-8376 and CVE-2024-10525
- Library OpenSSL: CVE-2024-9143 and CVE-2024-13176
- Library qt: CVE-2015-9541, CVE-2017-10904, CVE-2017-10905, CVE-2018-15518, CVE-2018-19869, CVE-2018-19870, CVE-2018-19871, CVE-2018-19873, CVE-2018-21035, CVE-2020-0569, CVE-2020-0570, CVE-2020-17507, CVE-2020-24742, CVE-2021-38593, CVE-2022-25634, CVE-2023-24607, CVE-2023-32573, CVE-2023-32762, CVE-2023-32763, CVE-2023-33285, CVE-2023-34410, CVE-2023-37369, CVE-2023-38197, CVE-2023-51714, CVE-2024-39936 and CVE-2025-30348
- Library zlib: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842 and CVE-2016-9843

Want to report a vulnerability or provide feedback – Please email us at secure@arcinfo.com

TLP:CLEAR



SECURITY BULLETIN

2025-1

ARC Informatique
Private limited company
capitalized at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C / SIREN 320 695 356
VAT N°FR 19320695 356

Headquarters
40 avenue Pierre Lefaucheux,
92100 Boulogne-Billancourt, France
Tel: +33 1 41 14 36 00
Hotline: +33 1 41 14 36 25
Email: arcnews@arcinfo.com
www.pcvue.com

ARC Informatique is
ISO 9001, ISO 14001 and
ISO 27001 certified

We would love to hear your thoughts and suggestions
so we can improve this document
Contact us at secure@arcinfo.com

TLP:CLEAR