SECURITY BULLETIN 2026-4

LIBRARIES UPDATES IN PCVUE 17.0.0

SUMMARY:

This document contains information about major updates of third-party libraries in PcVue Initial Release 17.0.0 since PcVue Feature Release 16.3.0.

Reference	SB2026-4
Publication date	2026.07.07
Last update	2026.07.07
Confidentiality	TLP:CLEAR

Date	Revision	Action
2026.07.07	1.0	Initial version

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 PcVue Initial Release 17.0.0 since PcVue Feature Release 16.3.0.

2. Affected libraries and components

Library/dependency	Affected components	Description
c-ares	PcVue	Bumped from version 1.34.4 to 1.34.5 It notably fixes CVE-2025-31498.
curl	PcVue	Bumped from version 8.15.0 to 8.16.0 It notably fixes CVE-2025-9086, CVE-2025-10148 and CVE-2025-10966
expat	ICCP add-on	Bumped from version 2.6.4 to 2.7.5 It notably fixes CVE-2024-8176, CVE-2025-59375, CVE-2026-24515, CVE-2026-25210, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778.
Google.Protobuf	PcVue	Bumped from version 3.31.0 to 3.33.0 It notably fixes CVE-2022-3171 and CVE-2025-47273.
libwebsockets	PcVue	Bumped from version 4.3.5 to 4.4.1 It notably fixes CVE-2025-11677.
libxml2	PcVue	Bumped from version 2.13.5 to 2.14.5 It notably fixes CVE-2024-56171, CVE-2025-24928, CVE-2025-27113, CVE-2025-32414 and CVE-2025-32415.

Library/dependency	Affected components	Description
mbed-TLS	PcVue	Bumped from version 3.6.2 to 3.6.5 It notably fixes : CVE-2025-27809, CVE-2025-27810, CVE-2025-47917, CVE-2025-48965, CVE-2025-49087, CVE-2025-49600, CVE-2025-49601, CVE-2025-52496 and CVE-2025-52497
openssl	PcVue	Bumped from version 3.5.2 to 3.5.4 It notably fixes It notably fixes CVE-2025-9230, CVE-2025-9231 and CVE-2025-9232

3. Impact

The impact on a particular system depends on many factors. According to the vulnerabilities described in this bulletin, users are responsible for assessing the potential impact of the identified vulnerabilities on their specific environment.

4. Immediate risk mitigation

Failure to implement the recommended updates or actions, including without limitation, recommended patches or remediations, shall be at user's sole risk and expense. The responsible entity shall take all appropriate actions to secure and safeguard its systems and data. ARC Informatique shall have no liability for failure to implement the recommended updates or actions or failure to secure and safeguard systems and data.

4.1 Harden the configuration

Who should apply this recommendation: All users

To reduce the risk of exploitation, ARC Informatique strongly recommends implementing the following defensive measures:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the insecure networks.
- Place 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.

Additional deployment guidance and recommended practices are available in the product documentation (Hardening Guide).

4.2 Update PcVue

Who should apply this recommendation: All users running affected components.

Apply the corrective update by installing PcVue Initial Release 17.0.0 or later

To verify that the patch is applied correctly, you must check that the *File version* property of the file *./bin/sv32.exe* matches release 17.0.0 (17.0.0902.3726) or later, and ensure that any earlier release is no longer used.

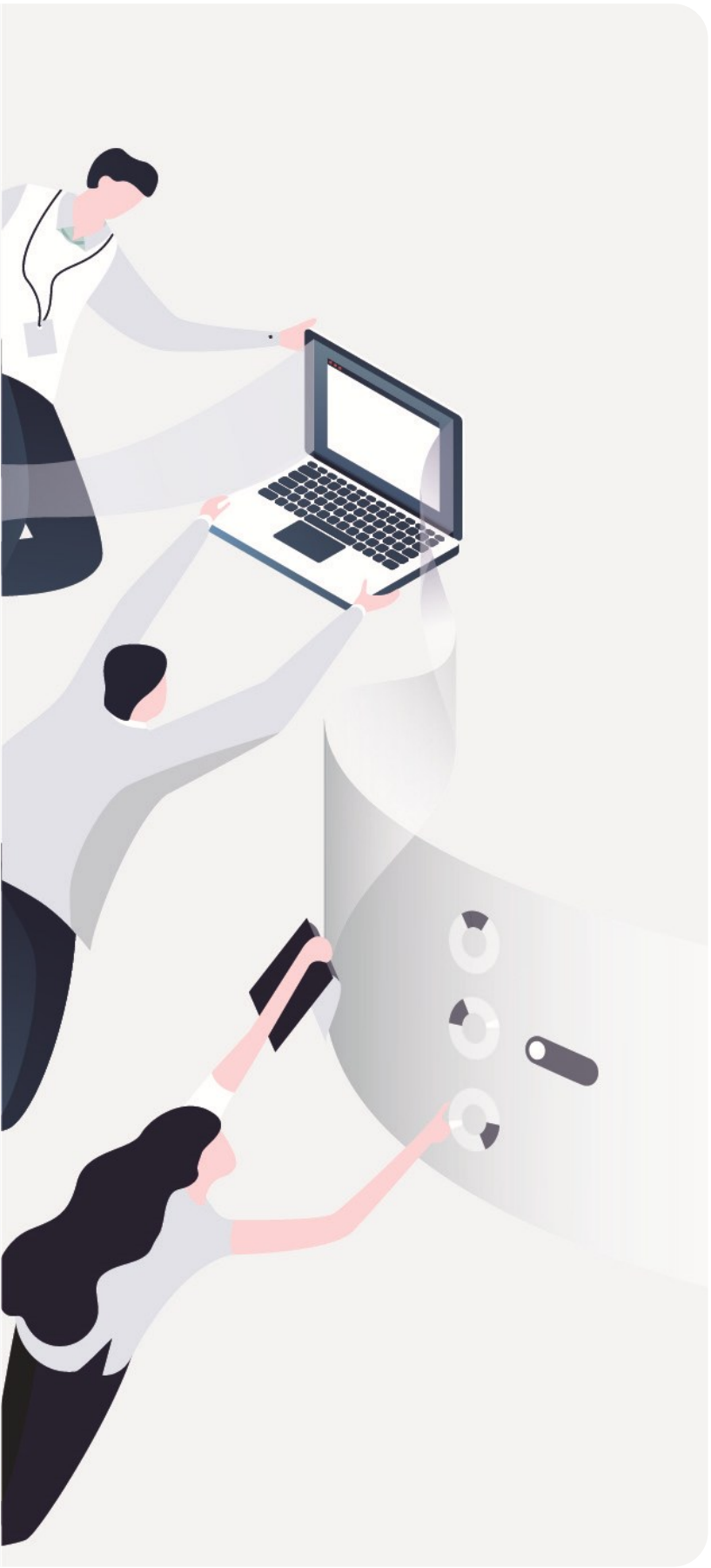
5. Credits

N/A

6. References

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

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



SECURITY BULLETIN

2026-4

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