SECURITY BULLETIN 2024-7

LIBRARIES UPDATES IN PCVUE 16.2.4

SUMMARY:

This document contains information about major updates of third-party libraries in PcVue 16.2.4.

Reference	SB2024-7
Publication date	2024.12.03
Last update	2024.12.03
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2024.12.03	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 Maintenance Release 16.2.4.

2. Affected libraries and components

Library/dependency	Affected components	Description
Bootstrap	WebVue	Updated from version 4.5.2 to 4.6.2 Multiple vulnerabilities
Dojo/Diji	WebVue	Updated from version 1.10.4 to 1.17.3 It notably fixes CVE-2010-2273, CVE-2018-15494, CVE-2020-5258, and CVE-2021-23450
jQuery	WebScheduler built-in help	Updated from version 1.8.3 to 3.7.1 It notably fixes CVE-2012-6708, CVE-2015-9251, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023 and CVE-2020-7656
libuv	PcVue – MQTT add-on	Updated to version 1.48.0 It notably fixes CVE-2024-24806
libxml2	PcVue	Updated from version 2.11.6 to 2.11.9 It notably fixes CVE-2024-25062
mbed-TLS	PcVue	Updated from version 2.28.5 to 3.6.1 It notably fixes CVE-2024-45157, and CVE-2024-28960
OpenSSL	PcVue – OPC UA driver PcVue – SNMP Manager driver PcVue – MQTT add-on	Updated from version 3.2.0 to 3.3.2 It notably fixes CVE-2024-6119, CVE-2024-5535, CVE-2024-4741, CVE-2024-4603, CVE-2024-2511, CVE-2024-0727, CVE-2023-6237, and CVE-2023-6129
Sentinel Super Pro	Remote License Manager PcVue	Updated from version 7.1.0.18 to 7.1.0.19 It includes updates of the expat library from version 2.6.2 to 2.6.3. It notably fixes CVE-2024-45490, CVE-2024-45491 and CVE-2024-45492
zlib	PcVue	Updated from version 1.3 to 1.3.1. It notably fixes CVE-2023-45853

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.
The older versions of the jQuery library are affected by multiple vulnerabilities, POC code exists, and some are known to be exploited by threat actors.

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. Credits

N/A

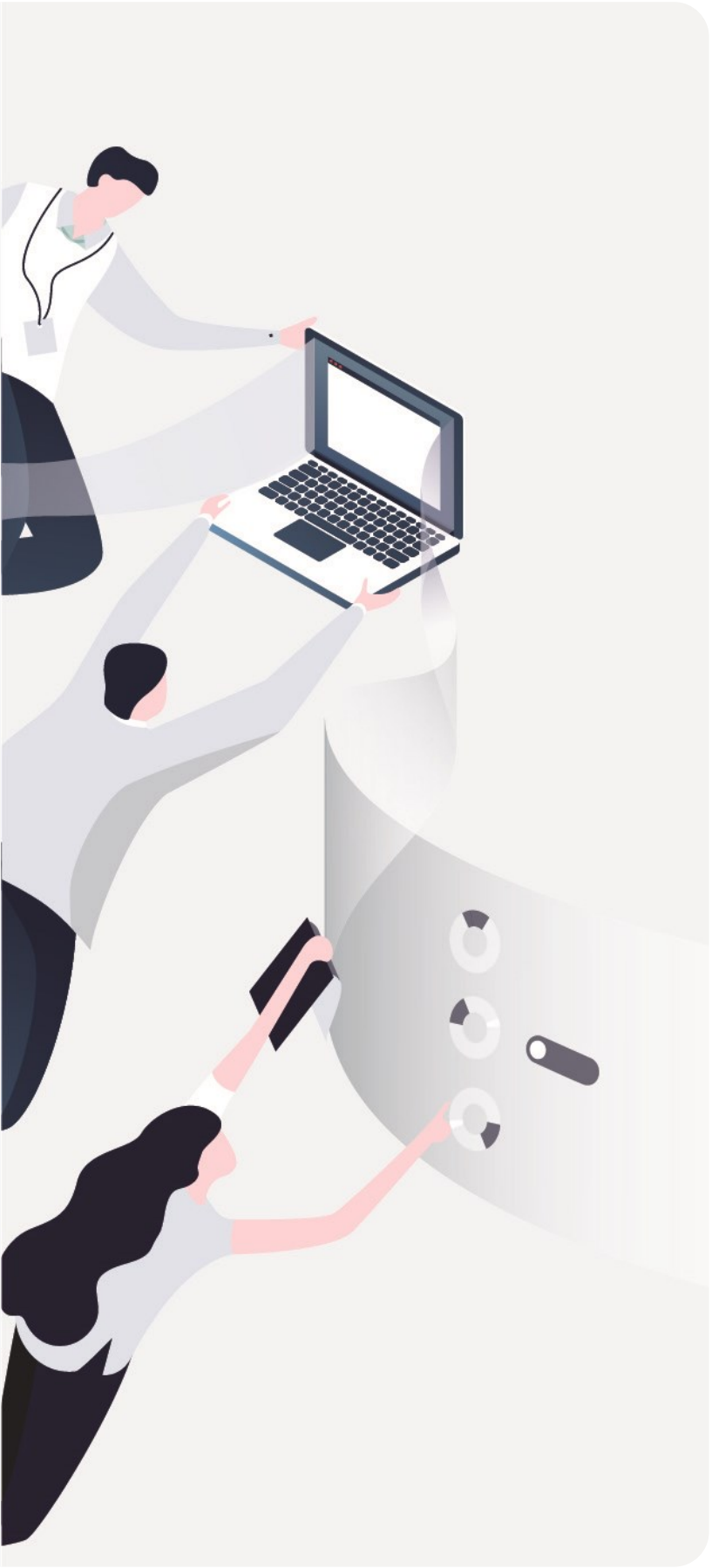
6. References

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

CVE:

- Library Dojo/Diji: CVE-2010-2273, CVE-2018-15494, CVE-2020-5258, and CVE-2021-23450
- Library jQuery: CVE-2012-6708, CVE-2015-9251, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023 and CVE-2020-7656
- Library libuv: CVE-2024-24806
- Library libxml2: CVE-2024-25062
- Library mbed-TLS: CVE-2024-45157, and CVE-2024-28960
- Library OpenSSL: CVE-2024-6119, CVE-2024-5535, CVE-2024-4741, CVE-2024-4603, CVE-2024-2511, CVE-2024-0727, CVE-2023-6237, and CVE-2023-6129
- Library Sentinel Super Pro: CVE-2024-45490, CVE-2024-45491 and CVE-2024-45492
- Library zlib: CVE-2023-45853

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



SECURITY BULLETIN

2024-7

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
2 avenue de la Cristallerie,
92310 Sèvres, 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