

SECURITY BULLETIN 2025-3

⚠ CERTIFICATE VALIDITY NOT PROPERLY VERIFIED

⚠ SUMMARY:

This document contains information about vulnerabilities affecting the MQTT add-on of PcVue.

Reference	SB2025-3
Publication date	2025.05.06
Last update	2025.05.06
Confidentiality	TLP:CLEAR

Date	Revision	Action
2025.05.06	1.0	Initial version

The information in this bulletin is subject to change without notice. The software described in this security bulletin is furnished under a license agreement and may only be used or copied in accordance with the terms of that agreement. It is against the law to copy software on any media except as specifically allowed in the license agreement. No part of this manual may be reproduced or transmitted in any form or by any means without the express permission of the publisher. The author and publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book. In particular, the information contained in this book does not substitute to the instructions from the products' vendor. This book may contain material belonging to third-parties. Such information is used exclusively in internal work processes and is not intended to be disclosed. In addition, this notice is not a claim of property on such third-party information. All product names and trademarks mentioned in this document belong to their respective owner.

1. Overview

ARC Informatique is aware of a security vulnerability affecting PcVue.

The vulnerable component is the MQTT add-on provided with PcVue. The vulnerability consists in an improper validation of certificate expiration.

2. Affected libraries and components

Component	Product & Versions	Description
MQTT add-on	PcVue 16 PcVue 15	Improper validation of a certificate expiration.

3. Impact

A malicious device could connect to the application and impersonate a legitimate device, injecting erroneous data.

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.

This vulnerability is not known to be exploited.

4. Vulnerability details

4.1 Denial of service attack

CVE Id	CVE-2025-4384
Publication date	2025.05.06
Description	The MQTT add-on of PcVue fails to verify that a remote device's certificate has not already expired or has not yet become valid. This allows malicious devices to present certificates that are not rejected properly. The use of a client certificate reduces the risk for random devices to take advantage of this flaw.
CVSS-B v4.0 Score	6.0
CVSS-B v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/E:A/AU:Y/R:U/RE:M/U:Green
CWE Id	CWE-298 : Improper Validation of Certificate Expiration

5. Immediate risk mitigation

5.1 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:

- Use client certificate when configuring the MQTT add-on.
- 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.

5.2 Update PcVue

Who should apply this recommendation: All users using the affected component

Apply the patch by installing a fixed PcVue version.

6. Available patches

Component	Vulnerability	Description
MQTT add-on	Improper Validation of Certificate Expiration	Patch provided with: • PcVue 16.3.0 Patch planned in: • PcVue 16.2.5 • PcVue 15.2.12

7. Credits

N/A

8. References

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

ARC Informatique's SPR Ids: SPR #70311

CVE:

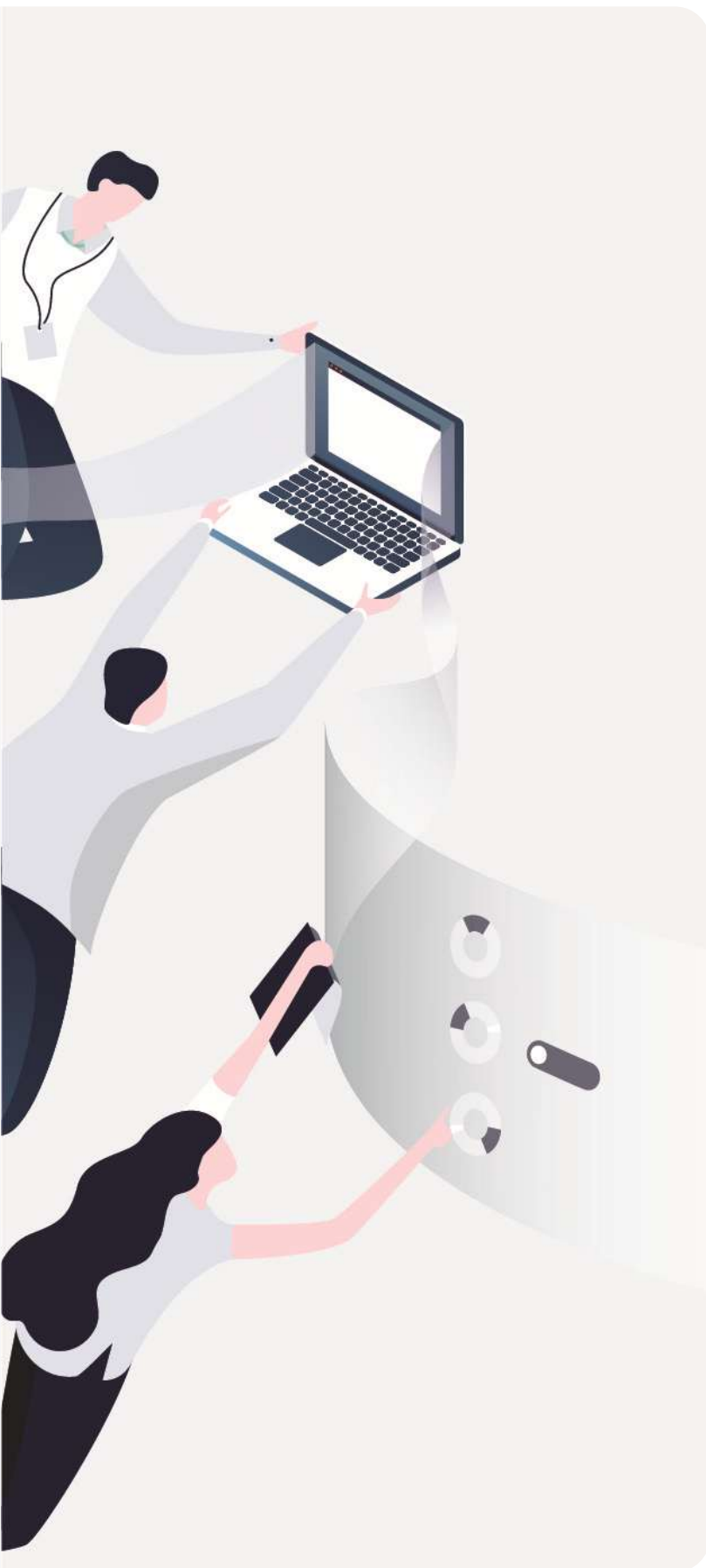
- [CVE-2025-4384](#)

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



SECURITY BULLETIN

2025-3



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 Lefauchaux
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