SECURITY BULLETIN 2023-4

MQTT pub/sub add-on vulnerabilities

SUMMARY :

This document contains information about a vulnerability affecting the MQTT pub/sub add-on.

Reference	SB2023-4
Publication date	2024.05.02
Last update	2024.07.04
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2024.05.02	1.0	Initial version
2024.07.04	Rev A	(editorial) Updated document template (technical) Updated section “Available patches” (fixed in PcVue 16.2.0)

1. Overview

ARC Informatique is aware of security vulnerabilities affecting PcVue.

The affected component is the Mosquitto library used for the MQTT pub/sub add-on. 2 vulnerabilities, listed below, have been reported in this library and affect PcVue:

- CVE-2023-0809: Excessive memory allocation
- CVE-2023-3592: Memory leak

This bulletin describes the immediate security measures to prevent the malicious exploitation of this vulnerability. We strongly recommend that users of the affected products apply these measures.

2. Affected products and components

Component	Product & Versions	Description
MQTT pub/sub add-on driver	All versions since PcVue 15.0	Use of a vulnerable version of the Mosquitto library

3. Impact

An attacker could remotely exploit those vulnerabilities by sending multiple messages which could lead to a Denial of Service.

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.

These vulnerabilities are not known to be exploited.

4. Vulnerability details

4.1 Excessive memory allocation

CVE Id	CVE-2023-0809			
Publication date	2023.02.10			
Description	In Mosquitto before 2.0.16, excessive memory is allocated based on malicious initial packets that are not CONNECT packets.			
CVSS v3.1 Base Score	5.8			
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L			
Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low		High	
Privileges Required	None	Low	High	
User interaction	None		Required	
Scope	Unchanged		Changed	
Confidentiality	None	Low	High	
Integrity	None	Low	High	
Availability	None	Low	High	
CWE Id	CWE-770: Allocation of Resources Without Limits or Throttling CWE-789: Memory Allocation with Excessive Size Value			

4.2 Memory leak

CVE Id	CVE-2023-3592			
Publication date	2023.02.10			
Description	In Mosquitto before 2.0.16, a memory leak occurs when clients send v5 CONNECT packets with a will message that contains invalid property types.			
CVSS v3.1 Base Score	5.8			
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L			
Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low		High	
Privileges Required	None	Low	High	
User interaction	None		Required	
Scope	Unchanged		Changed	
Confidentiality	None	Low	High	
Integrity	None	Low	High	
Availability	None	Low	High	
CWE Id	CWE-401: Missing Release of Memory after Effective Lifetime			

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:

- 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 pub/sub add-on	Use of a vulnerable version of the Mosquitto library	Fixed in: • PcVue 16.1.2 • PcVue 16.2.0

7. Credits

N/A

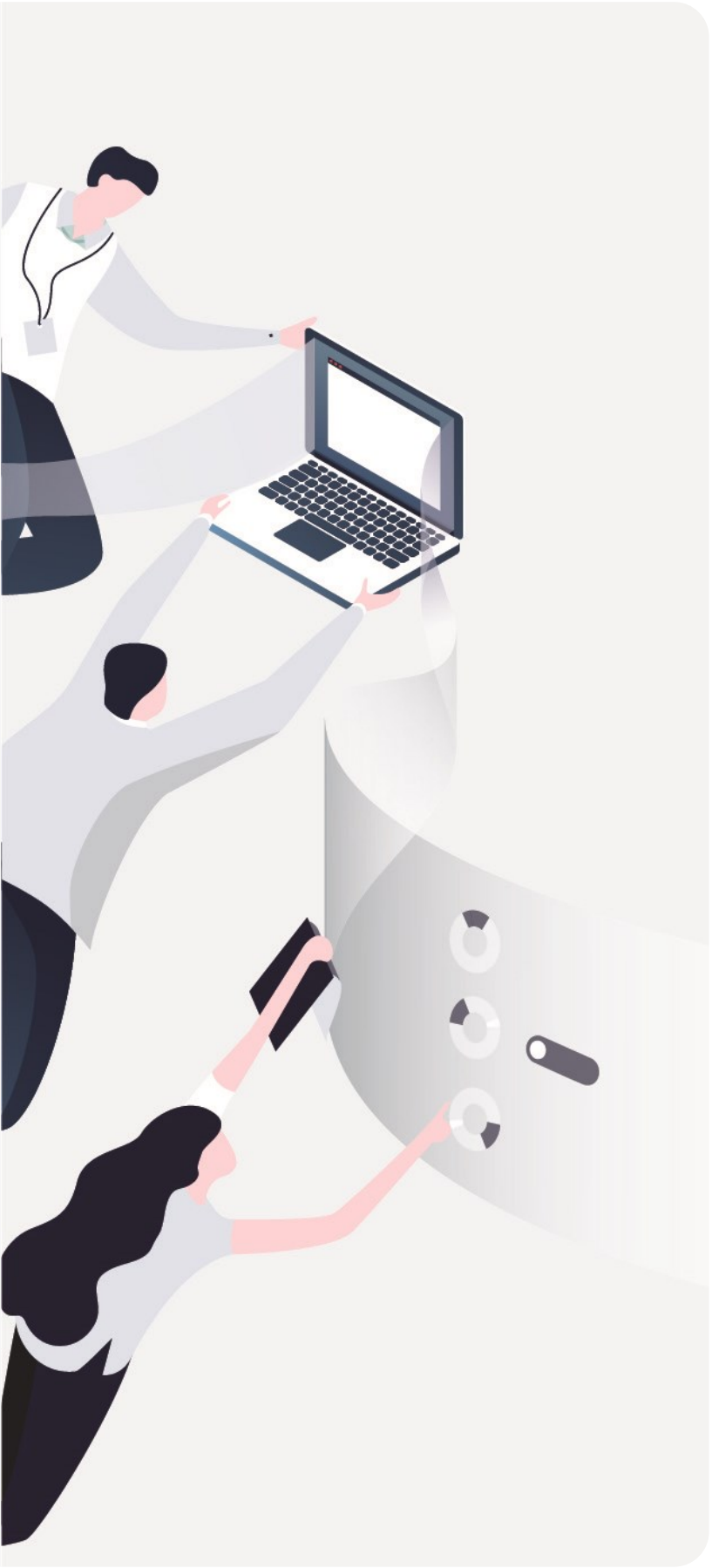
8. References

The public ARC Informatique security alert page: www.pcvuesolutions.com

CVE:

- CVE-2023-0809
- CVE-2023-3592

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



SECURITY BULLETIN

2023-4

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
2 avenue de la Cristallerie,
92310 Sèvres, France
Tél: +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