SECURITY BULLETIN 2024-8

⁞ IEC 61850 CLIENT DRIVER & ICCP ADD-ON VULNERABILITY

⁞ SUMMARY:

This document contains information about a vulnerability affecting the IEC 61850 client driver and the ICCP add-on.

Reference	SB2024-8
Publication date	2025.03.21
Last update	2025.03.21
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2025.03.17	1.0	Initial version

1.   Overview

ARC Informatique is aware of a security vulnerability affecting PcVue.

The affected components are the IEC 61850 client driver and the ICCP client add-on in PcVue. The vulnerability consists in an incorrect processing of response messages in the Triangle MicroWork's IEC 61850 & ICCP Client library.

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
IEC 61850 client driver	All versions since PcVue 10.0	The vulnerability is related to the incorrect processing of response messages that are formatted to be sent to servers when received by a client after sending a request. This incorrect processing can cause a fatal error resulting in a denial of service.
ICCP add-on	All versions since PcVue 15.1	

This vulnerability only affects the ICCP add-on when configured in client-only mode. It does not affect it when configured as a server or when configured for bi-directional communication.

3.   Impact

This incorrect message processing can cause a fatal error resulting in 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 evaluates the risk for their system.

This vulnerability is not known to be exploited.

4. Vulnerability details

4.1 Incorrect message processing

CVE Id	In progress			
Publication date	YYYY.MM.DD			
Description	The vulnerability is related to the incorrect processing of response messages that are formatted to be sent to servers when received by a client after sending a request. This incorrect processing can cause a fatal error resulting in a denial of service.			
CVSS v3.1 Base Score	8.2			
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H			
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-476: NULL Pointer Dereference			

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

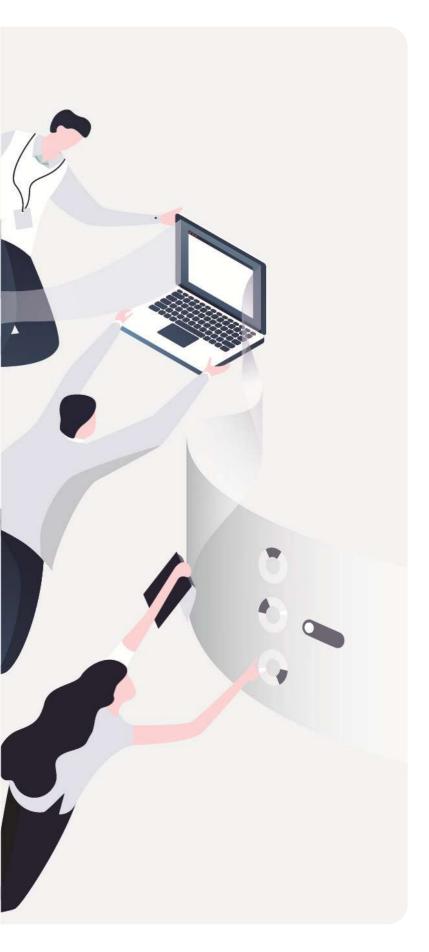| Component	Vulnerability	Description
IEC 61850 client driver	Incorrect message processing	Fixed in: • PcVue 16.2.4 • PcVue 15.2.11
ICCP add-on	Incorrect message processing	Planned in: • PcVue 16.2.5 • PcVue 15.2.12

7.   Credits

N/A

8.   References

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

ARC Informatique's SPR Id: SPR #74471

CVE: In progress

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

SECURITY BULLETIN

2024-8

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