SECURITY BULLETIN 2024-1

IEC 61850 CLIENT VULNERABILITY

SUMMARY :

This document contains information about a vulnerability affecting the IEC 61850 client driver.

Reference	SB2024-1
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 a security vulnerability affecting PcVue.

The affected component is the IEC 61850 client driver in PcVue. The vulnerability consists in a Buffer Overflow in the Triangle MicroWork's IEC 61850 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	A Buffer overflow vulnerability has been identified resulting from specially crafted MMS messages. The vulnerability is related to the absence of a buffer size check when processing received messages which can allow a buffer overrun.

3. Impact

This buffer overflow 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 evaluate the risk for their system.

This vulnerability is not known to be exploited.

4. Vulnerability details

4.1 Buffer overflow

CVE Id	In progress			
Publication date	YYYY.MM.DD			
Description	A vulnerability has been identified in the TMW IEC 61850 Client libraries resulting from specially crafted MMS messages. This vulnerability has been present in the software libraries since their initial release. The effected libraries include the C, C++, .Net, and Java versions of IEC 61850 Client libraries released before February of 2024. The vulnerability is related to the absence of a buffer size check when processing received messages which can allow a buffer overrun. This buffer overflow can cause a crash 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-120: Buffer Copy without Checking Size of Input			

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	Buffer overflow	Fixed in: • PcVue 15.2.9 • PcVue 16.1.2 • PcVue 16.2.0 Planned in: • PcVue 12.0.30

7. Credits

N/A

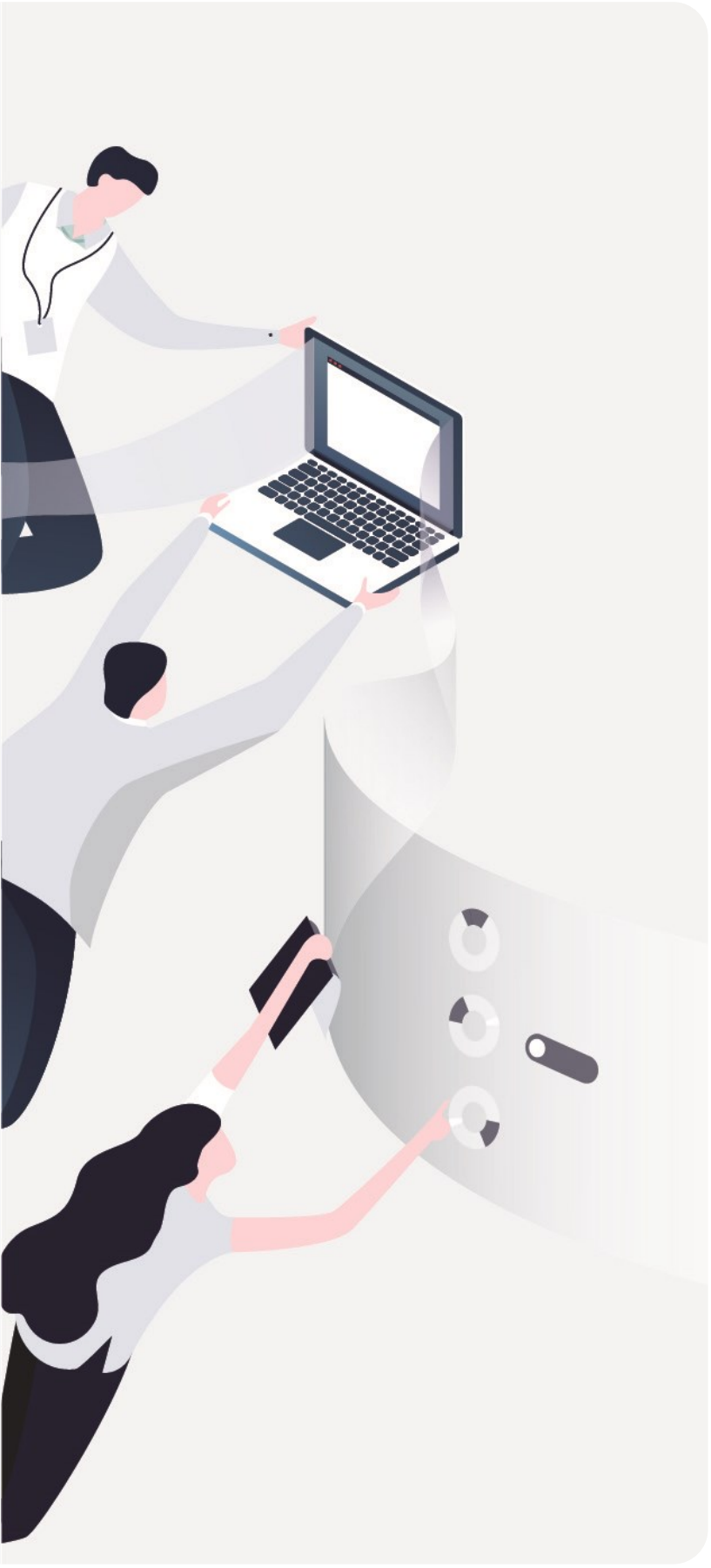
8. References

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

ARC Informatique's SPR Id: SPR #73486

CVE: *Assignment in progress*

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



SECURITY BULLETIN

2024-1

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