Security Bulletin 2022-5

IEC 61850 client driver and ICCP/TASE.2 interface vulnerabilities

Publication date :	19/09/2022
Last update :	19/09/2022
Document revision :	1.0

Content of the document : This document contains information about vulnerabilities affecting the IEC 61850 client driver and ICCP/TASE.2 interface.

Overview

ARC Informatique is aware of a security vulnerability affecting PcVue. The affected components are the IEC 61850 client driver and ICCP/TASE.2 interface.
This bulletin describes the immediate security measures to prevent the malicious exploitation of these vulnerabilities. We strongly recommend that users of the affected products apply these measures.

Affected products and components

Component	Product	Description
IEC 61850 client driver	PcVue - From version 10.0 onward	An Access of Uninitialized Pointer vulnerability exists in the stack used for the IEC 61850 client driver.
ICCP/TASE.2 interface	PcVue - From version 15.1 onward	An Access of Uninitialized Pointer vulnerability exists in the stack used for the ICCP/TASE.2 interface.

Impact

An attacker can leverage these vulnerabilities by targeting the IEC 61850 client driver or ICCP/TASE.2 interface. Successful exploitation of these vulnerabilities could lead to a denial-of-service condition of the targeted system. Note that the affected software needs to be running for these vulnerabilities to be exploited. Vulnerable hosts are typically data acquisition servers or ICCP gateways.

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.

Vulnerability details

1. Access to Uninitialized Pointer

CVE-IDS	CVE-2022-38138
Publication date	2022.09.06
Description	The TMW IEC 61850 Library and TMW 60870-6 (ICCP/TASE.2) Library are vulnerable to access given to a small number of uninitialized pointers. This could allow an attacker to target any client or server using the affected libraries to cause a denial-of-service condition.
Impact	Successful exploitation of this vulnerability could lead to a denial-of-service condition.
CVSS v3.1 Base Score	7.5
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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	824 – Access of Uninitialized Pointer

Mitigation

1. Harden the configuration

Who should apply this recommendation: All users
The affected components are TCP client and server interfaces. You should make sure incoming and outgoing connections on the corresponding ports are authorized. The users 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.
- 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.

2. Update PcVue

Who should apply this recommendation: All users using the affected component
Apply the patch by installing a fixed PcVue version.

Available patches

Component	Vulnerability	Product
IEC 61850 client driver	Access to Uninitialized Pointer	Fixed in: - PcVue 15.2.3 A fix for PcVue 12 is planned
ICCP/TASE.2 interface	Access to Uninitialized Pointer	Fixed in: - PcVue 15.2.3 A fix for PcVue 12 is planned

References

The public ARC Informatique security alert page: www.pcvuesolutions.com
This security bulletin on the Technical Resources web site

CVE: CVE-2022-38138

ICS CERT advisory: ICS Advisory (ICSA-22-249-01)

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

Document history

Revision	Action	Date
Version 1.0	First publication	19/09/2022

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 19320695356

Security Bulletin 2022-5

ISO 9001 and ISO 14001 certified

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

We would love to hear your thoughts and suggestions
so we can improve this document
Contact us at secure@pcvuesolutions.com