Security Bulletin 2024-1

IEC 61850 client vulnerability

TLP:CLEAR

Publication date:	2024.05.02
Last update:	2024.05.02
Document revision:	1.0
Content of the document:	This document contains information about a vulnerability affecting the IEC 61850 client driver.

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.

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.

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.

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.

Vulnerability details

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.			
Impact	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			

Immediate risk mitigation

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.

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

Credits

N/A

References

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

ARC Informatique's SPR Id: SPR #73486

CVE: CVE-2024-xxx (assignment in progress)

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

Revision history

Revision	Action	Date
Version 1.0	Initial version	2024.05.02

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

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 2024-1

© Copyright 2024. All rights reserved.
Partial or integral reproduction is
prohibited without prior authorization.
All names and trademarks are the
property of their respective owners.

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@pcvuesolutions.com