Security Bulletin 2022-7

Email & SMS accounts configuration vulnerability

Publication date:	25/11/2022
Last update:	23/01/2023
Document revision:	1.0 Rev C
Content of the document:	This document contains information about a vulnerability affecting the configuration of the email & SMS accounts.

Overview

ARC Informatique is aware of a security vulnerability affecting PcVue.
The affected component is the configuration of the email & SMS accounts in PcVue. The vulnerability consists in Cleartext Storage of Sensitive Information due to connection secrets being stored in plain text in a configuration file of the project.
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	Description
Email accounts configuration	All versions since PcVue 8.10	Cleartext Storage of Sensitive Information vulnerability, allowing a user able to authenticate locally to access the SMTP account credentials.
SMS accounts configuration	All versions since PcVue 8.10	Cleartext Storage of Sensitive Information vulnerability, allowing a user able to authenticate locally to access the SIM card PIN code.

Impact

By exploiting the vulnerability, an attacker could access the email account.
Successful exploitation of this vulnerability could lead to unauthorized access to the underlying email account and SIM card.

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. Cleartext Storage of Sensitive Information

CVE Id	CVE-2022-4312
Publication date	2022.12.12
Description	A Cleartext Storage of Sensitive Information vulnerability exists in PcVue since version 8.10, allowing a user able to authenticate locally to access email & SMS accounts configuration, and in particular the SMTP account credentials and the SIM card PIN code.
Impact	Successful exploitation of this vulnerability could lead to an unauthorized access to the underlying email account and SIM card.
CVSS v3.1 Base Score	5.5
Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
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	312 - Cleartext Storage of Sensitive Information

Immediate risk mitigation

1. Harden the configuration

Who should apply this recommendation: All users
You should make sure project files are only accessible to authorized 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.
- 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. By doing so, PcVue will protect SMTP account credentials and SIM card PIN codes in the corresponding configuration file.

Available patches

Component	Vulnerability	Product
Email account configuration	Cleartext Storage of Sensitive Information	Fixed in: - PcVue 15.2.4 - PcVue 12.0.28
SMS account configuration	Cleartext Storage of Sensitive Information	Fixed in: - PcVue 15.2.4 - PcVue 12.0.28

Credits

ARC Informatique thanks the product user for reporting and coordinated disclosure.

References

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

CVE: CVE-2022-4312

ICS-CERT advisory: ICSA-22-354-03

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	25/11/2022
Version 1.0 Rev A	Added CVE Id in *Vulnerability details* and *References*	20/12/2022
Version 1.0 Rev B	Added ICS-CERT advisory in *References*	21/12/2022
Version 1.0 Rev C	Updated fixed versions in *Available patches* section	23/01/2023

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 2022-7

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