Security Bulletin 2022-4

OAuth configuration vulnerability

Publication date:	08/08/2022
Last update:	19/09/2022
Document revision:	1.0 Rev A
Content of the document:	This document contains information about a vulnerability affecting the configuration of the OAuth web service.

Overview

ARC Informatique is aware of a security vulnerability affecting PcVue.
The affected component is the configuration of the OAuth web service hosted in Microsoft IIS. The vulnerability consists in Cleartext Storage of Sensitive Information due to a connection string being stored in plain text in a configuration file of the service.
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
OAuth web service configuration	PcVue 12 PcVue 15	A Cleartext Storage of Sensitive Information vulnerability exists, allowing a user able to authenticate locally to access session data of legitimate users stored in the OAuth database.

Impact

By exploiting the vulnerability, an attacker could access the OAuth web service database.
Successful exploitation of the vulnerability may have the following impact:

- Exposure of data from sessions corresponding to users connected via WebVue, the WebScheduler or the mobile apps. The issue may also affect any deployed 3rd party systems based on the Web Services Toolkit.
- Prevent legitimate users to connect and operate properly if using WebVue, the WebScheduler or the mobile apps. The issue may also affect any deployed 3rd party systems based on the Web Services Toolkit.

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-2022-2569
Publication date	2022.08.08
Description	A Cleartext Storage of Sensitive Information vulnerability exists in PcVue 12 & 15, allowing a user able to authenticate locally to access session data of legitimate users stored in the OAuth database.
Impact	Exposure of data from sessions corresponding to users connected via WebVue, the WebScheduler or the mobile apps. The issue may also affect any deployed 3rd party systems based on the Web Services Toolkit. Prevent legitimate users to connect and operate properly if using WebVue, the WebScheduler or TouchVue mobile apps. The issue may also affect any deployed 3rd party systems based on the Web Services Toolkit.
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

Mitigation

1. Uninstall the Web Server

Who should apply this recommendation: All users not using the affected component
The OAuth web service and its configuration are part of the Web Server for PcVue. If your system does not require the use of the Web & Mobile features, you should make sure not to install them. See the product help related to the installation for more information.

2. Update the Web Deployment Console and re-deploy the Web Server

Who should apply this recommendation: All users using the affected component
Install a patched release of product, including the Web Deployment Console (WDC) and use the WDC to re-deploy the Web Server. By doing so, the WDC will update and protect the database connection string, including clearing any sensitive information stored in the web.config file.

Available patches

Component	Vulnerability	Product
OAuth web service configuration	Cleartext Storage of Sensitive Information	Fixed in: - PcVue 12.0.27 - PcVue 15.2.3

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-2022-2569
ICS-CERT advisory: ICSA-22-235-01

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	08/08/2022
Version 1.0 Rev A	Added availability of the fix for version 15 in 15.2.3 Improved explanation related to updating the WDC ICS-CERT advisory published – Ref added	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 2022-4

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