SECURITY BULLETIN 2024-4

IMPROPERLY IMPLEMENTED SECURITY CHECK IN OAUTH WEB SERVICE

SUMMARY:

This document contains information about a vulnerability affecting the OAuth server of PcVue.

Reference	SB2024-4
Publication date	2024.12.02
Last update	2024.12.02
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2024.12.02	1.0	Initial version

1. Overview

ARC Informatique is aware of a security vulnerability affecting PcVue.

The affected component is the OAuth server of PcVue. The vulnerability consists in an incorrect implementation of the Client secret check for the Password Grant type as defined in the OAuth v2.0 standard.

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
OAuth web service	PcVue 12.0 to PcVue 16.2.0	The Client secret is not checked when using the Password grant type.

3. Impact

By exploiting this vulnerability, an attacker could connect to a web server using a client application not explicitly authorized as part of the OAuth deployment.
Exploitation requires valid credentials and does not permit the attacker to bypass user privileges.

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 evaluates the risk for their system.

This vulnerability is not known to be exploited.

4. Vulnerability details

4.1 Improperly implemented security check

CVE Id	CVE-2024-12056
Publication date	2024.12.02
Description	The Client secret is not checked when using the OAuth Password grant type. By exploiting this vulnerability, an attacker could connect to a web server using a client application not explicitly authorized as part of the OAuth deployment. Exploitation requires valid credentials and does not permit the attacker to bypass user privileges.
CVSS v4.0 Base Score	2.3
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N/AU:N/R:U/RE:M/U:Green
CWE Id	CWE-358: Improperly Implemented Security Check for Standard

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 Uninstall the Web Server

Who should apply this recommendation: All users **not** using the affected component
The OAuth web service is 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.

5.3 Update the Web Deployment Console (WDC) 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.

6. Available patches

Component	Vulnerability	Description
OAuth web service	Improperly Implemented Security Check	Fixed in: • PcVue 16.2.1

7. Credits

N/A

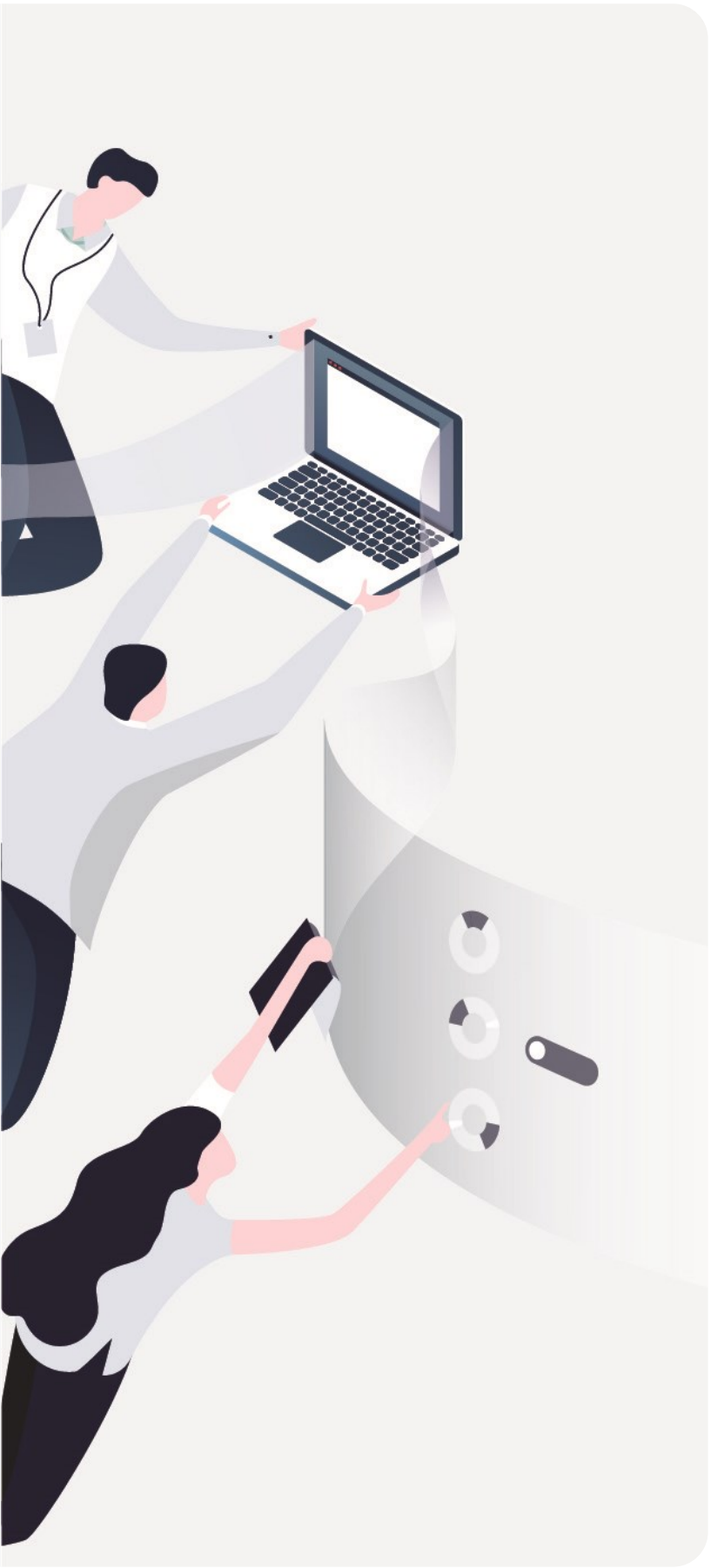
8. References

The public ARC Informatique security alert page: www.pcvue.com/security

ARC Informatique's SPR Id: SPR #73326

CVE: CVE-2024-12056

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



SECURITY BULLETIN

2024-4

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
Tel: +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