Security Bulletin 2022-6

Sensitive Information in Log File vulnerability

Publication date:	19/09/2022
Last update:	19/09/2022
Document revision:	1.0
Content of the document:	This document contains information about a vulnerability affecting the confidentiality of connection strings of the DbConnect.

Overview

ARC Informatique is aware of a security vulnerability affecting PcVue.
The vulnerability consists in an Insertion of Sensitive Information into Log File. Specifically, connection strings to data sources for the DbConnect, including credentials, could be found in log files when the log level is set to its highest level.
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
Log Files	PcVue 15	An Insertion of Sensitive Information into Log File vulnerability exists, allowing a user with access to the log files to discover connection strings of the data sources configured for the DbConnect, including the credentials.

Impact

By exploiting the vulnerability, an attacker could access the data sources configured for the DbConnect. Successful exploitation of this vulnerability could lead to an unauthorized access to the underlying data sources.

Note that the log level of the affected component has to be set to its highest level for this vulnerability to be exploited.

The exact impact on a particular system depends on many factors, in particular privileges associated with the credentials and the nature of the data stored in the data sources. 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. Insertion of Sensitive Information into Log File

CVE Id	Not yet assigned
Publication date	Not yet published
Description	An Insertion of Sensitive Information into Log File vulnerability exists, allowing a user with access to the log files to discover connection strings of the data sources configured for the DbConnect, including the credentials.
Impact	Successful exploitation of this vulnerability could lead to an unauthorized access to the underlying data sources.
CVSS v3.1 Base Score	4.7
Vector	CVSS:3.1/AV:L/AC:H/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	532 - Insertion of Sensitive Information into Log File

Mitigation

1. Minimize log level

Who should apply this recommendation: All users

Deactivate the log level "Trace 2: Configuration" on the Sql Connections configured in your project (if any). If this log level was activated in your project, make sure to protect or delete existing local log files found in the folder <InstallDir>\Bin\Log Files.

In general, only activate the necessary log details. Detailed levels are designed for diagnostics (as opposed to general events logging) and should only be activated when necessary.

2. Harden the configuration

Who should apply this recommendation: All users

You should make sure Log 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.

3. Update PcVue

Who should apply this recommendation: All users using the affected component
Apply the patch by installing a fixed PcVue version. Connection strings are no longer visible in the log files whatever the log level is.

Available patches

Component	Vulnerability	Product
Log File	Insertion of Sensitive Information into Log File	Fixed in: - PcVue 15.2.3

References

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

CVE: Not yet published

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

PcVue Solutions

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 2022-6

swiss safety center
ISO 9001
ISO 14001
certified system

ISO 9001 and ISO 14001 certified

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