

# SECURITY BULLETIN 2026-5

## ➤ MULTIPLE VULNERABILITIES AFFECTING THE USER ACCOUNTS CONFIGURATION

### ➤ SUMMARY:

This document contains information about vulnerabilities affecting the configuration of User accounts in PcVue.

|                  |                  |
|------------------|------------------|
| Reference        | SB2026-5         |
| Publication date | 2026.07.07       |
| Last update      | 2026.07.07       |
| Confidentiality  | <b>TLP:CLEAR</b> |

| Date       | Revision | Action          |
|------------|----------|-----------------|
| 2026.07.07 | 1.0      | Initial version |

The information in this document is subject to change without notice. The software described in this document 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 document 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 document. In particular, the information contained in this document does not substitute to the instructions from the products' vendor. This document 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.

## 1. Overview

ARC Informatique is aware of security vulnerabilities affecting PcVue.

The vulnerable component is the configuration of User accounts and the protection of the association configuration file. The vulnerabilities are described hereinafter.

## 2. Affected libraries and components

| Component                   | Product & Versions | Description                                  |
|-----------------------------|--------------------|----------------------------------------------|
| User accounts configuration | All PcVue versions | Insecure password storage in User directory  |
|                             |                    | Weak encryption mechanism for User directory |

## 3. Impact

By exploiting these vulnerabilities, an attacker could potentially retrieve credentials of built-in user accounts, alter permissions of existing users or create new users, and ultimately gain privileged access to the PcVue application.

At the time of writing, these vulnerabilities are not known to be exploited.



The impact on a particular system depends on many factors. According to the vulnerabilities described in this bulletin, users are responsible for assessing the potential impact of the identified vulnerabilities on their specific environment.

## 4. Vulnerability details

### 4.1 Insecure password storage in User directory

|                  |                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE Id           | <a href="#">CVE-2026-14867</a>                                                                                                                                                                                                                                 |
| Publication date | 2026.07.07                                                                                                                                                                                                                                                     |
| Description      | <p>Credentials of built-in users are insecurely stored in the User directory of PcVue projects, all versions prior to 17.0.0. A local attacker could retrieve users' credentials.</p> <p>Active Directory accounts are not affected by this vulnerability.</p> |
| CVSS-B Score     | 6.8                                                                                                                                                                                                                                                            |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/AU:Y/R:U/RE:M/U:Amber</a>                                                                                                                                                          |
| CWE Id           | <a href="#">CWE-256</a> : Plaintext Storage of a Password                                                                                                                                                                                                      |

### 4.2 Weak encryption mechanism for User directory

|                  |                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE Id           | <a href="#">CVE-2026-14868</a>                                                                                                                                                                                                                                                                                                                                |
| Publication date | 2026.07.07                                                                                                                                                                                                                                                                                                                                                    |
| Description      | <p>The encryption algorithm used to protect the configuration of user accounts, stored in the built-in user directory of PcVue projects, all versions prior to 17.0.0, is not strong enough for the level of protection required. A local attacker could alter the existing configuration and ultimately gain privileged access to the PcVue application.</p> |
| CVSS-B Score     | 8.4                                                                                                                                                                                                                                                                                                                                                           |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/AU:Y/R:U/RE:M/U:Amber</a>                                                                                                                                                                                                                                                         |
| CWE Id           | <a href="#">CWE-326</a> : Inadequate Encryption Strength                                                                                                                                                                                                                                                                                                      |

## 5. Immediate risk mitigation



Failure to implement the recommended updates or actions, including without limitation, recommended patches or remediations, shall be at user's sole risk and expense. The responsible entity shall take all appropriate actions to secure and safeguard its systems and data. ARC Informatique shall have no liability for failure to implement the recommended updates or actions or failure to secure and safeguard systems and data.

### 5.1 Harden the configuration

Who should apply this recommendation: All users

To reduce the risk of exploitation, ARC Informatique strongly recommends implementing the following defensive measures:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the insecure networks.
- 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.

Additional deployment guidance and recommended practices are available in the product documentation ([Hardening Guide](#)).

### 5.2 Update PcVue

Who should apply this recommendation: All users using the affected component

Apply the corrective update by installing PcVue Initial Release 17.0.0 or later

In a patched release, it will no longer be possible to load User directory from earlier versions. Existing projects designed with an earlier version require explicit migration using the ProjectUtility CLI tool. Instructions are provided in the product documentation ([Project Utility CLI reference](#)).

To verify that the patch is applied correctly, you must check that the *File version* property of the file `./bin/sv32.exe` matches release 17.0.0 (17.0.0902.3726) or later, and ensure that any earlier release is no longer used.

## 6. Available patches

| Component                   | Vulnerability                                | Description                                                                                          |
|-----------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------|
| User accounts configuration | Insecure password storage in User directory  | Patch provided with: <ul style="list-style-type: none"><li>• PcVue 17.0.0 (17.0.0902.3726)</li></ul> |
|                             | Weak encryption mechanism for User directory |                                                                                                      |

## 7. Credits

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

## 8. References

The public ARC Informatique security alert page: [www.pcvue.com/security](http://www.pcvue.com/security)

ARC Informatique's SPR Ids:

SPR #75977, 76690, 76015

CVE:

- [CVE-2026-14867](#), [CVE-2026-14868](#)

Want to report a vulnerability or provide feedback – Please email us at [secure@arcinfo.com](mailto:secure@arcinfo.com)



# SECURITY BULLETIN

## 2026-5

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  
40 avenue Pierre Lefauchaux  
92100 Boulogne-Billancourt, France  
Tel: +33 1 41 14 36 00  
Hotline: +33 1 41 14 36 25  
Email: [arcnews@arcinfo.com](mailto:arcnews@arcinfo.com)  
[www.pcvue.com](http://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](mailto:secure@arcinfo.com)