SECURITY BULLETIN 2025-4

MULTIPLE VULNERABILITIES IN THE NETWORKING FEATURE

SUMMARY:

This document contains information about vulnerabilities affecting the TCP-based client/server Networking feature of PcVue.

Reference	SB2025-4
Publication date	2025.09.05
Last update	2026.02.25
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2025.09.05	1.0	Initial version
2025.10.31	Rev A	(technical) Updated sections “Overview”, “Immediate risk mitigation”, “Available patches” and “References” following the discovery of a regression in patched releases.
2026.02.25	Rev B	(technical) Updated sections “Overview”, “Immediate risk mitigation” and “Available patches”.

1. Overview

ARC Informatique is aware of security vulnerabilities affecting PcVue.

The vulnerable component is the TCP-based client/server Networking feature provided with PcVue. The vulnerabilities consist in a Denial of Service (DoS) attack and in an improper validation of the payloads.

Rev A: The previously announced patched releases, PcVue 12.0.31, 15.2.12 and 16.3.2, are affected by a regression in the TCP-based client/server Networking feature causing connection instability.
Rev B: The regression in the TCP-based client/server Networking feature is fixed in PcVue 12.0.32, and 15.2.13.

2. Affected libraries and components

Component	Product & Versions	Description
Networking	All PcVue versions up to 16.3.0 (included)	Networking packets sequencing was not correctly checked. Reception of specially crafted messages could force the application to stop.
Networking	All PcVue versions up to 16.3.0 (included)	Payload elements were not correctly checked, allowing an attacker to execute unauthorized commands in the application.

3. Impact

By exploiting these vulnerabilities, an attacker could potentially access the PcVue host and its filesystem or run arbitrary code, and also take control of the PcVue process or force it to stop. Exploitation requires access to the local network where the system is deployed, knowledge of the payload structures, the specific Networking configuration and IP addresses.

In addition, these vulnerabilities may prove to be very complex to exploit if defensive measures to minimize the host and network exposure are in place:

- Network perimeter firewalls properly configured to filter the traffic on the TCP-based networking ports,

- And local firewalls on PcVue hosts properly configured to limit traffic on these ports to the PcVue main process only.

These measures highly hinder the potential for exploitation.

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 Improper validation of packets sequencing

CVE Id	CVE-2025-9998
Publication date	2025.09.05
Description	The sequence of packets received by a Networking server are not correctly checked. An attacker could exploit this vulnerability to send specially crafted messages to force the application to stop.
CVSS-B Score	6.0
CVSS-B Vector	CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/E:A/AU:Y/R:U/RE:M/U:Green
CWE Id	CWE-754: Improper Check for Unusual or Exceptional Conditions

4.2 Improper validation of payload elements

CVE Id	CVE-2025-9999
Publication date	2025.09.05
Description	Some payload elements of the messages sent between two stations in a networking architecture are not properly checked on the receiving station allowing an attacker to execute unauthorized commands in the application.
CVSS-B Score	7.6
CVSS-B Vector	CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green
CWE Id	CWE-940: Improper Verification of Source of a Communication Channel CWE-1288: Improper Validation of Consistency within Input

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 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 Update PcVue

Initial version:

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

~~Apply the patch by installing a fixed PcVue version.~~

~~A fixed release must be installed on all stations. Any attempt to establish a connection between a station running a release with the fix and a station without it will fail.~~

Rev A:

~~The previously announced releases, PcVue 12.0.31, 15.2.12 and 16.3.2, are affected by a regression in the TCP-based client/server Networking feature causing connection instability. If the security fix is enabled, networking packets can be falsely detected as malformed, causing a server station to force a disconnection. This issue leads to a situation where a client station may not be able to stay connected to a server station in a stable way.~~

~~We recommend users having installed PcVue 12.0.31, 15.2.12 or 16.3.2 to either roll back to an earlier stable release, or to disable this mechanism by:~~

- ~~Check the security alteration setting named *'Networking.Allow security altering configuration options'*,~~
- ~~Set the property *'Allow stations with altered security'* on Nodes to Yes.~~

Rev B:

Who should apply this recommendation: All users running affected components.

Apply the patch by installing a fixed PcVue version.

A fixed release must be installed on all stations for the fix to be fully applied.

Existing projects require a settings update for the fix to be applied. The complete update procedure and verification steps are described in the Knowledge Base article KB1254.

For new projects, the settings are configured by default with secured values.

To verify that the patch is applied correctly, the user must check that:

- The *File version* property of the file *./bin/sv32.exe* matches the deployed release or later, and ensure that any earlier release is no longer used;
- The *Interoperability issues* settings of the Networking feature are disabled.

6. Available patches

Component	Vulnerability	Description
Networking	Improper validation of packets sequencing	Patch provided in: • PcVue 16.3.4 (16.3.4902.3112) • PcVue 15.2.13 (15.2.13902.37126) • PcVue 12.0.32 (12.0.32900.37130)
	Improper validation of payload elements	

Rev A: remove list of patched release, added list of newly planned releases

Rev B: updated list of patched release, including the fix for the previously mentioned regression.

7. Credits

ARC Informatique thanks Guillaume André and Pierre Gertner from Synacktiv for reporting and coordinated disclosure.

8. References

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

ARC Informatique's Knowledge Base article:

KB1254

ARC Informatique's SPR Ids:

SPR #74709, 74710 and 74711

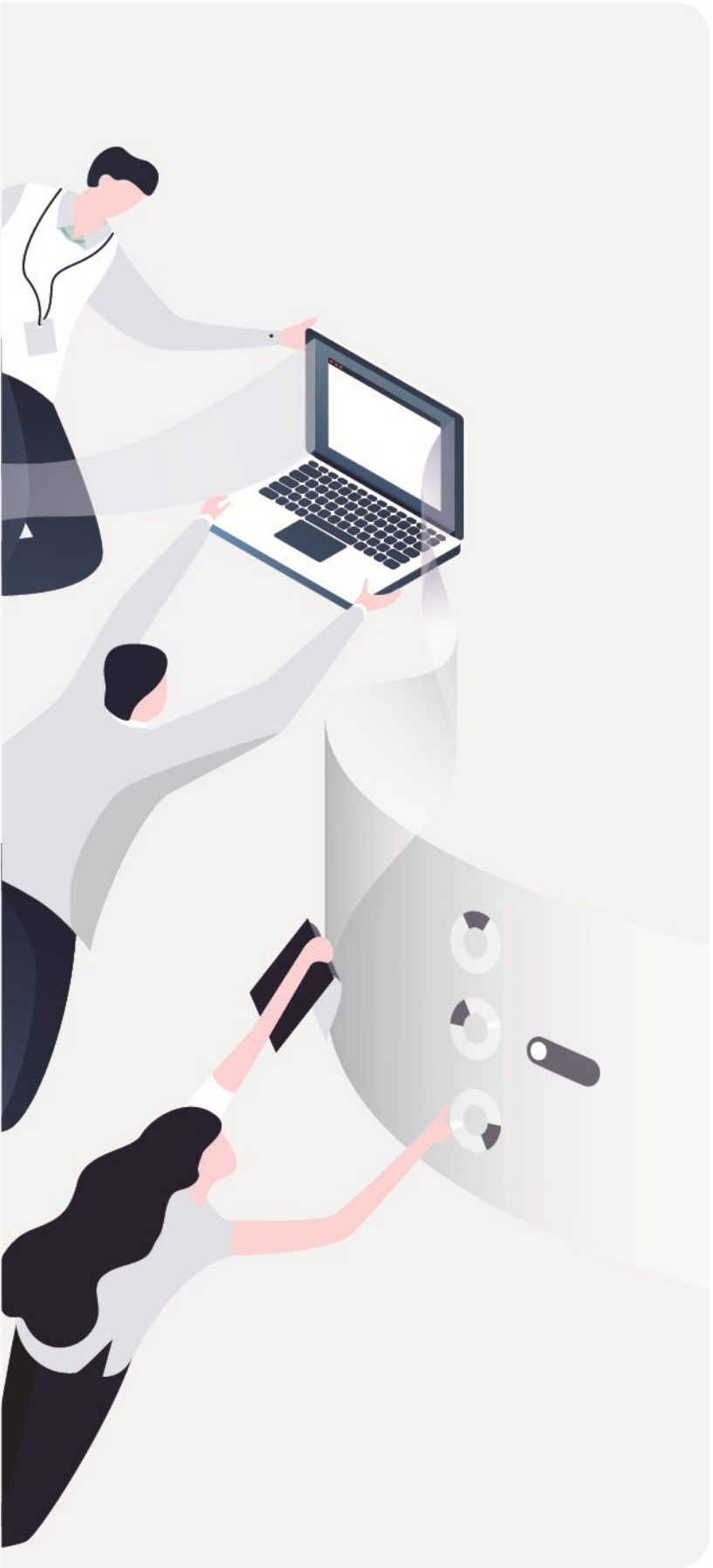
Rev A: SPR #76112

CVE:

- CVE-2025-9998
- CVE-2025-9999

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

TLP:CLEAR



SECURITY BULLETIN

2025-4

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
40 avenue Pierre Lefaucheux
92100 Boulogne-Billancourt, 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

TLP:CLEAR