

# SECURITY BULLETIN 2026-2

## › MULTIPLE VULNERABILITIES AFFECTING WEB SERVICES AND WEB APPS

### › SUMMARY:

This document contains information about vulnerabilities affecting the web services and web apps of PcVue, including the WebVue, WebScheduler, TouchVue and SnapVue feature.

|                  |                  |
|------------------|------------------|
| Reference        | SB2026-2         |
| Publication date | 2026.02.26       |
| Last update      | 2026.03.26       |
| Confidentiality  | <b>TLP:CLEAR</b> |

| Date       | Revision | Action  |
|------------|----------|---|
| 2026.02.25 | 1.0      | Initial version                                 |
| 2026.03.26 | Rev A    | (technical) Updated section “Available patches” |

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 components are the web services and web apps provided with PcVue. The vulnerabilities are described hereinafter.

## 2. Affected libraries and components

| Component    | Product & Versions                         | Description  |
|--------------|--|--|
| WebVue       | All PcVue versions since 12.0.0 (included) | Missing origin validation in GraphicalData web service requests                      |
| WebScheduler |  | Use of vulnerable Resource Owner Password Credentials flow                           |
| TouchVue     |  | Server configuration details in HTTP headers   |
| SnapVue      |  | XSS vulnerability upon unsuccessful authentication                                   |
| Web services |  | Missing security HTTP headers  |
| WebVue       | All PcVue versions since 12.0.0 (included) | Use of unsecure cookies for the GraphicalData web service and the WebClient web apps |
| WebVue       | All PcVue versions since 15.0.0 (included) | HTTP Host header vulnerability in the WebClient and WebScheduler web app             |

## 3. Impact

By exploiting these vulnerabilities, an attacker could potentially access the IIS Web server and its filesystem, run arbitrary code, or intercept sensitive information or user credentials.

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 Missing origin validation in GraphicalData web service requests

|                  |   |
|------------------|---|
| CVE Id           | <a href="#">CVE-2026-1692</a>   |
| Publication date | 2026.02.26  |
| Description      | <p>A missing origin validation in WebSockets vulnerability affects the GraphicalData web services used by the WebVue, WebScheduler, TouchVue and SnapVue features of PcVue in version 12.0.0 through 16.3.3 included. It might allow a remote attacker to lure a successfully authenticated user to a malicious website.</p> <p>This vulnerability only affects the following two endpoints:<br/>GraphicalData/js/signalR/connect and GraphicalData/js/signalR/reconnect.</p> |
| CVSS-B Score     | 5.3   |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N/AU:Y/RE:M/U:Clear</a>   |
| CWE Id           | <a href="#">CWE-1385</a> : Missing Origin Validation in WebSockets  |

### 4.2 Use of vulnerable Resource Owner Password Credentials flow

|                  |  |
|------------------|--|
| CVE Id           | <a href="#">CVE-2026-1693</a>  |
| Publication date | 2026.02.26   |
| Description      | <p>The OAuth grant type Resource Owner Password Credentials (ROPC) flow is still used by the web services used by the WebVue, WebScheduler, TouchVue and Snapvue features of PcVue in version 12.0.0 through 16.3.3 included despite being deprecated. It might allow a remote attacker to steal user credentials.</p> |
| CVSS-B Score     | 5.3  |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green</a>  |
| CWE Id           | <a href="#">CWE-1390</a> : Weak Authentication<br><a href="#">CWE-477</a> : Use of Obsolete Function   |

### 4.3 Server configuration details in HTTP headers

|                  |   |
|------------------|---|
| CVE Id           | <a href="#">CVE-2026-1694</a>   |
| Publication date | 2026.02.26  |
| Description      | HTTP headers are added by the default configuration of IIS and ASP.net, and are not removed at the deployment phase of the webservices used by the WebVue, WebScheduler, TouchVue and SnapVue features of PcVue in version 12.0.0 through 16.3.3 included. It unnecessarily exposes sensitive information about the server configuration. |
| CVSS-B Score     | 2.3   |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/AU:Y/R:U/RE:M/U:Green</a>   |
| CWE Id           | <a href="#">CWE-201</a> : Insertion of Sensitive Information into Sent Data   |

### 4.4 XSS vulnerability upon unsuccessful authentication

|                  |  |
|------------------|--|
| CVE Id           | <a href="#">CVE-2026-1695</a>  |
| Publication date | 2026.02.26   |
| Description      | An XSS vulnerability affects the OAuth web services used by the WebVue, WebScheduler, TouchVue and SnapVue features of PcVue in version 12.0.0 through 16.3.3 included. It might allow a remote attacker to trick a legitimate user into loading content from another site upon unsuccessful user authentication on an unknown application (unknown client_id).<br><br>This vulnerability only affects the error page of the OAuth server. |
| CVSS-B Score     | 5.3  |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green</a>  |
| CWE Id           | <a href="#">CWE-79</a> : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')  |

### 4.5 Missing security HTTP headers

|                  |   |
|------------------|---|
| CVE Id           | <a href="#">CVE-2026-1696</a>   |
| Publication date | 2026.02.26  |
| Description      | Some HTTP security headers are not properly set by the web server when sending responses to the client application. |
| CVSS-B Score     | 2.3   |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green</a>               |
| CWE Id           | <a href="#">CWE-79</a> : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')       |

### 4.6 Use of unsecure cookies for GraphicalData web service and WebClient web app

|                  |  |
|------------------|--|
| CVE Id           | <a href="#">CVE-2026-1697</a>  |
| Publication date | 2026.02.26   |
| Description      | The Secure and SameSite attribute are missing in the GraphicalData web services and WebClient web app of PcVue in version 12.0.0 through 16.3.3 included.              |
| CVSS-B Score     | 5.3  |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green</a>  |
| CWE Id           | <a href="#">CWE-614</a> : Sensitive Cookie in HTTPS Session Without 'Secure' Attribute<br><a href="#">CWE-1275</a> : Sensitive Cookie with Improper SameSite Attribute |

## 4.7 HTTP Host header vulnerability in WebClient and WebScheduler web apps

|                  |   |
|------------------|---|
| CVE Id           | <a href="#">CVE-2026-1698</a>   |
| Publication date | 2026.02.26  |
| Description      | <p>A HTTP Host header attack vulnerability affects WebClient and the WebScheduler web apps of PcVue in version 15.0.0 through 16.3.3 included, allowing a remote attacker to inject harmful payloads that manipulate server-side behavior.</p> <p>This vulnerability only affects the endpoints /Authentication/ExternalLogin, /Authentication/AuthorizationCodeCallback and /Authentication/Logout of the WebClient and WebScheduler web apps.</p> |
| CVSS-B Score     | 5.3   |
| CVSS-B Vector    | <a href="#">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green</a>   |
| CWE Id           | <a href="#">CWE-644</a> : Improper Neutralization of HTTP Headers for Scripting Syntax  |

## 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 unsecure 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.

## 5.2 Uninstall the Web Server

Who should apply this recommendation: All users **not** using the affected component

If your system does not require the use of the Web & Mobile features, you should make sure not to install them. If your system requires the use of the Web & Mobile features, they should be installed only on the Web Server.

See the product help related to the installation for more information.

## 5.3 Update IIS configuration – manually update HTTP headers

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

As a quick mitigation for the unnecessary and missing HTTP headers, you can disable default headers and add secure HTTP headers for all requests. Those options can be set via the web.config file located on the IIS by following those steps:

- 1) Open the file `C:\inetpub\<SV Website>\web.config`
- 2) Add the following entries to the section `customHeaders`, which are the recommendations from the official OWASP site:

```
<remove name="X-Powered-By" />
<add name="X-Frame-Options" value="DENY" />
<add name="X-XSS-Protection" value="0" />
<add name="X-Content-Type-Options" value="nosniff" />
<add name="X-DNS-Prefetch-Control" value="off" />
<add name="Cross-Origin-Opener-Policy" value="same-origin" />
<add name="Cross-Origin-Embedder-Policy" value="require-corp" />
<add name="Cross-Origin-Resource-Policy" value="same-site" />
<add name="Referrer-Policy" value="strict-origin-when-cross-origin" />
<add name="Strict-Transport-Security" value="max-age=63072000; includeSubDomains; preload" />
<add name="Permissions-Policy" value="geolocation=(), camera=(), microphone=()" />
```

## 5.4 Update IIS configuration – disable caching

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

As a quick mitigation for the caching control, you can set the caching header directly for all requests with the IIS manager. This will ensure that no sensitive data is cached, but it will also disable the caching of other resources which should normally be cached (i.e., images).

Disabling the cache can be done by following this procedure:

<https://learn.microsoft.com/en-us/iis/configuration/system.webserver/staticcontent/clientcache#how-to-disable-caching-for-a-web-site-or-application>

## 5.5 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 the Web Deployment Console (WDC) on the IIS Web server and use it to re-deploy the Web Site. Some settings might need to be updated if third-party web apps or services depend on the OAuth ROPC flow.

In a patched release of the WDC, new settings are available for each authorized Client to enable or disable:

- The Authorization Code flow
- The Authorization Code flow with PKCE
- The Resource Owner Password Credentials (ROPC) flow

By default, all the OAuth flows are now disabled for third-party web apps and need to be manually enabled before deployment if required.

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

- The *File version* property of the file `./bin/Modules/WebDeployment/WebDeploymentConsole.exe` matches the deployed release or later, and ensure that any earlier release is no longer used;
- Web Sites have been redeployed;
- OAuth flow are correctly set for each authorized Client.

## 6. Available patches

| Component    | Vulnerability   | Description   |
|--------------|---|---|
| WebVue       | Missing origin validation in GraphicalData web service requests                     | Patch provided with:<br><ul style="list-style-type: none"> <li>• PcVue 16.3.4 (16.3.4902.3112)</li> <li>• PcVue 15.1.14 (15.2.14900.37147)</li> </ul> |
| WebScheduler | Use of vulnerable Resource Owner Password Credentials flow                          |   |
| TouchVue     | Server configuration details in HTTP headers  |   |
| SnapVue      | XSS vulnerability upon unsuccessful authentication                                  |   |
| Web services | Missing security HTTP headers   |   |
| WebVue       | Use of unsecure cookies for the GraphicalData web service and the WebClient web app |   |
| WebVue       | HTTP Host header vulnerability in the WebClient and WebScheduler web apps           |   |

Rev A: updated list of patched release

## 7. Credits

ARC Informatique thanks the product user 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 #74709,74889, 76369, 76370, 76372, 76373, 76374, 76374, 76375, 76376, 76378, 76379 and 76380

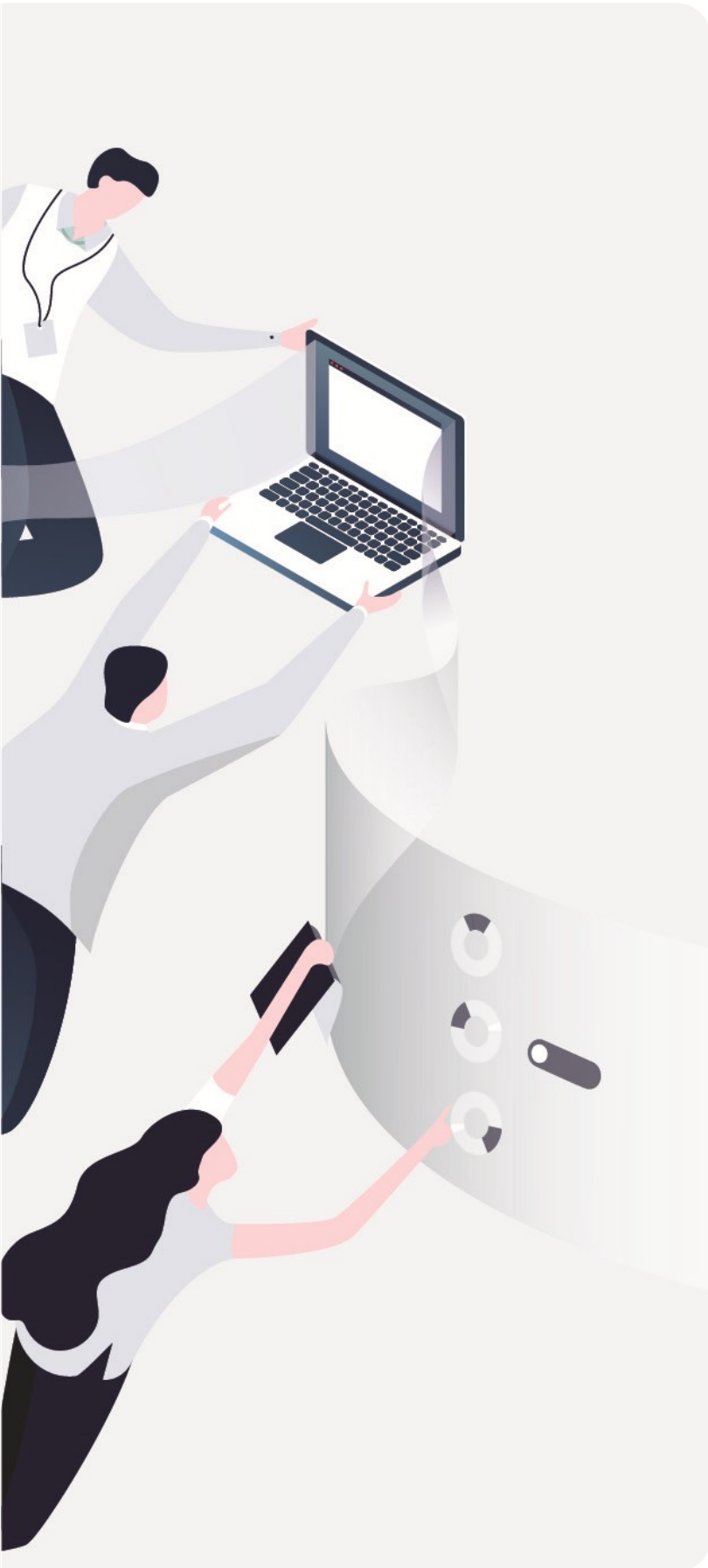
CVE:

- [CVE-2026-1692](#), [CVE-2026-1693](#), [CVE-2026-1694](#), [CVE-2026-1695](#), [CVE-2026-1696](#), [CVE-2026-1697](#), [CVE-2026-1698](#)

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



# SECURITY BULLETIN 2026-2



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)