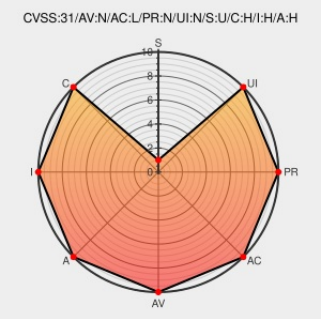
CVE-2020-26867

Published on: 10/12/2020 12:00:00 AM UTC

Last Modified on: 10/19/2022 05:26:00 PM UTC

CVE-2020-26867 - advisory for ICSA-20-308-03

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pcvue from Pcvuesolutions contain the following vulnerability:

ARC Informatique PcVue prior to version 12.0.17 is vulnerable due to the deserialization of untrusted data, which may allow an attacker to remotely execute arbitrary code on the web and mobile back-end server.

CVE-2020-26867 has been assigned by vulnerability@kaspersky.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **ARC Informatique** - **PcVue** version **<= 12.0.17**

Vulnerability Patch/Work Around

The following mitigations and workarounds have been identified by ARC Informatique to help reduce risk: Uninstall the web and mobile backend. Users not using the affected components should uninstall them. If the components are not required, do not install them. Change default configuration if using components prior to v12.0. If taking advantage of the web and mobile back features with a product version up to v11.2, change the following configuration item manually to prevent remote code execution In the file \Bin\PropertyServer.config>, change the following element and set it to “Low” (defaults to “Full”): This workaround cannot be applied to PcVue v12.0 Harden firewall configuration by ensuring that incoming connections on the corresponding port are authorized only if initiated by the IIS Web Server process. The listening port is configurable (default 8090) and may have been changed on the system using the Application Explorer.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ARC Informatique PcVue | CISA	us-cert.cisa.gov text/html	MISC us-cert.cisa.gov/ics/advisories/icsa-20-308-03
KLCERT-20-015: Remote Code Execution in ARC Informatique PcVue | Kaspersky ICS CERT	ics-cert.kaspersky.com text/html	CONFIRM ics-cert.kaspersky.com/advisories/klcert-advisories/2020/10/09/klcert-20-015-remote-code-execution-in-arc-informatique-pcvue/
Security bulletin	www.pcvuesolutions.com text/html Inactive Link Not Archived	CONFIRM www.pcvuesolutions.com/support/index.php/en/security-bulletin/1076-security-bulletin-2020-1
Security Alerts | PcVue Solutions	www.pcvuesolutions.com text/html	CONFIRM www.pcvuesolutions.com/security

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pcvuesolutions	Pcvue	All	All	All	All
Application	Pcvuesolutions	Pcvue	All	All	All	All

cpe:2.3:a:pcvuesolutions:pcvue:*:*:*:*:*:*:*:*:

cpe:2.3:a:pcvuesolutions:pcvue:*:*:*:*:*:*:*:*:

Discovery Credit

Sergey Temnikov and Andrey Muravitsky of Kaspersky Lab reported these vulnerabilities to ARC Informatique.

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Php - CVE-2020-26867: us-cert.cisa.gov/ics/advisories…	2022-10-19 19:03:12

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report