Security Bulletin 2020-1

Property Server vulnerabilities

Publication date :	05/10/2020
Last update :	29/07/2021
Document revision :	1.0 Rev E
Content of the document :	This document contains information about 3 vulnerabilities affecting the Web & Mobile back end interface.

Overview

ARC Informatique is aware of security vulnerabilities affecting PcVue.
The affected component is the interface between the Web & Mobile back end and the web services hosted in Microsoft IIS. Vulnerabilities consist in Remote Code Execution, Denial Of Service and Information exposure.
We have been working in coordination with the security researchers who reported these vulnerabilities.
This bulletin describes the immediate security measures to prevent the malicious exploitation of these vulnerabilities. We strongly recommend that users of the affected products apply these measures.
[Rev E] Following the initial fixes released in October 2020, additional tests have uncovered more ways to exploit similar Remote Code Execution vulnerabilities.

Affected products and components

Component	Product	Description
Property Server	PcVue - From version 8.10 onward	A Remote Code Execution vulnerability exists due to the unsafe deserialization of messages received on the interface. Related to CVE-2014-1806.
Property Server	PcVue – From version 12 Initial Release (12.0.7) onward	A Denial Of Service vulnerability exists due to the ability for a non-authorized user to modify information used to validate messages sent by legitimate web clients.
Property Server	PcVue – From version 12 Initial Release (12.0.7) onward	An information exposure vulnerability exists, allowing a non-authorized user to access session data of legitimate users.

Impact

By connecting to the interface and interacting with the server, an attacker can leverage these vulnerabilities on the targeted system. Note that the affected software needs to be running for this vulnerability to be exploited.

Successful exploitation of these vulnerabilities may have the following impact:

- Execution of an arbitrary process on the Web & Mobile back end server,
- Prevent legitimate users to connect and operate properly if using WebVue, the WebScheduler or the TouchVue mobile app. The issue also affects 3rd party systems based on the Web Services Toolkit.
- Exposure of data from sessions corresponding to users connected via WebVue, the WebScheduler or the TouchVue mobile app. The issue also affects 3rd party systems based on the Web Services Toolkit.

The exact impact on a particular system depends on many factors. According to the vulnerabilities described hereafter, we recommend that each user of the affected products evaluate the risk for their system.

Vulnerability details

1. Remote Code Execution

CVE-IDS	CVE-2020-26867
Publication date	2020.10.07
Researcher	Sergey Temnikov and Andrey Muravitsky from Kaspersky Lab
Description	A Remote Code Execution vulnerability exists in PcVue from version 8.10 onward, due to the unsafe deserialization of messages received on the interface.
Impact	Execution of an arbitrary process on the Web & Mobile back end server
CVSS v3.1 Base Score	9.8
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
Exploitability	Remote~~/Local~~
Difficulty	Low/~~Medium/High~~
User interaction	None~~/Yes~~
Existence of exploit	~~Unknown~~/PoC/~~Exploit~~

2. Denial Of Service

CVE-IDS	CVE-2020-26868
Publication date	2020.10.07
Researcher	Sergey Temnikov and Andrey Muravitsky from Kaspersky Lab
Description	A Denial Of Service vulnerability exists in PcVue 12, due to the ability for a non-authorized user to modify information used to validate messages sent by legitimate web clients.
Impact	Prevent legitimate users to connect and operate properly if using WebVue, the WebScheduler or the TouchVue mobile app. The issue also affects 3rd party systems based on the Web Services Toolkit.
CVSS v3.1 Base Score	7.5
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
Exploitability	Remote~~/Local~~
Difficulty	Low/~~Medium/High~~
User interaction	None~~/Yes~~
Existence of exploit	~~Unknown~~/PoC/~~Exploit~~

3. Session information exposure

CVE-IDS	CVE-2020-26869
Publication date	2020.10.07
Researcher	Sergey Temnikov and Andrey Muravitsky from Kaspersky Lab
Description	An information exposure vulnerability exists in PcVue 12, allowing a non-authorized user to access session data of legitimate users.
Impact	Exposure of data from sessions corresponding to users connected via WebVue, the WebScheduler or the TouchVue mobile app. The issue also affects 3rd party systems based on the Web Services Toolkit.
CVSS v3.1 Base Score	7.5
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
Exploitability	Remote~~/Local~~
Difficulty	Low/~~Medium/High~~
User interaction	None~~/Yes~~
Existence of exploit	~~Unknown~~/PoC/~~Exploit~~

Immediate risk mitigation

The Property Server interface should not be exposed directly. Taking advantage of Web & Mobile clients only requires the IIS Web Server to be able to access it. Therefore, we recommend you to immediately apply the following measures.

1. Uninstall the Web & Mobile back end

Who should apply this recommendation: All users not using the affected component
The Property Server is part of the Web & Mobile extensions of PcVue. If your system does not requires the use of the Web & Mobile features, you should make sure not to install them. In all cases, Web & Mobile extensions should only be installed on the PcVue Web back end server.
See the product help related to the installation for more information.

2. Harden your firewall configuration

Who should apply this recommendation: All users
The affected component is a TCP server interface. You should make sure incoming connections on the corresponding port are authorized only if initiated by your IIS Web Server process.
Up until version 11.2, the affected component and the IIS Web Server were deployed on the same machine. Any remote connection on this port can be blocked.
The listening port is configurable (default 8090) and may have been changed on your system using the Application Explorer (Communication.Servers.Web & Mobile back end).

Available patches

Component	Vulnerability	Product
Property Server	Remote Code Execution	Initial fix in: - PcVue 12.0.17 - PcVue 11.2.06097 [Rev E] Additional fix in: - PcVue 15.1.2 - PcVue 12.0.23 - PcVue 11.2.06100
Property Server	Denial Of Service	Fixed in: - PcVue 12.0.17
Property Server	Session information exposure	Fixed in: - PcVue 12.0.17

Credits

ARC Informatique thanks Sergey Temnikov and Andrey Muravitsky from Kaspersky Lab for reporting and coordinated disclosure.

References

The public ARC Informatique security alert page: www.pcvuesolutions.com
This security bulletin on the Technical Resources web site
CVE: CVE-2020-26867, CVE-2020-26868, CVE-2020-26869
Kasperky Lab advisories: KLCERT-20-015, KLCERT-20-016, KLCERT-20-017
ICS-CERT advisory: ICSA-20-308-03
CERT-FR advisory: CERTFR-2020-AVI-685

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	05/10/2020
Version 1.0 Rev A	CVE Id added (publication in progress)	08/10/2020
Version 1.0 Rev B	CVE published – Ref added Kaspersky advisories published – Ref added	13/10/2020
Version 1.0 Rev C	ICS-CERT & CERT-FR advisories published – Refs added	05/11/2020
Version 1.0 Rev D	Changes related to version 11.2: - Only the RCE vulnerability affects version earlier than 12.0. The 2 other vulns only affect version 12.0 – Affected versions updated. - Changing default configuration cannot be employed as a mitigation method – Paragraph removed (TypeFilterLevel). - Fix available for PcVue 11.2 – Release build added.	01/12/2020
Version 1.0 Rev E	Additional fixes against the RCE available for PcVue 11.2, 12 and 15 – Release builds added.	28/07/2021

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
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 2020-1

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