SECURITY BULLETIN 2023-3

OpenSSL vulnerabilities

SUMMARY :

This document contains information about vulnerabilities in the OpenSSL library.

Reference	SB2023-4
Publication date	2024.05.02
Last update	2024.07.04
Confidentiality	**TLP:CLEAR**

Date	Revision	Action
2024.05.02	1.0	Initial version
2024.07.04	Rev A	(editorial) Updated document template (technical) Updated section “Available patches” (fixed in PcVue 16.2.0) (technical) Removed CVE-2022-4304 from the affected items

1. Overview

ARC Informatique is aware of security vulnerabilities affecting PcVue.

The affected component is the OpenSSL library used in PcVue for the following features:

- OPC UA
- SNMP v3
- MQTT

Multiple vulnerabilities, listed below, have been reported on this library. Those that might affect the product are highlighted.

Affected	CVE Id	Title
	CVE-2022-1292	The c_rehash script allows command injection
	CVE-2022-2068	The c_rehash script allows command injection
	CVE-2022-2097	AES OCB fails to encrypt some bytes
	CVE-2022-4304	Timing Oracle in RSA Decryption
	CVE-2022-4450	Double free after calling PEM_read_bio_ex
	CVE-2023-0215	Use-after-free following BIO_new_NDEF
	CVE-2023-0286	X.400 address type confusion in X.509 GeneralName
	CVE-2023-0464	Excessive Resource Usage Verifying X.509 Policy Constraints
	CVE-2023-0465	Invalid certificate policies in leaf certificates are silently ignored
	CVE-2023-0466	Certificate policy check not enabled
	CVE-2023-1255	Input buffer over-read in AES-XTS implementation on 64 bit ARM
	CVE-2023-2650	Possible DoS translating ASN.1 object identifiers
	CVE-2023-2975	AES-SIV implementation ignores empty associated data entries
	CVE-2023-3446	Excessive time spent checking DH keys and parameters
	CVE-2023-3817	Excessive time spent checking DH q parameter value
X	CVE-2023-4807	POLY1305 MAC implementation corrupts XMM registers on Windows
	CVE-2023-5363	Incorrect cipher key & IV length processing
X	CVE-2023-5678	Excessive time spent in DH check / generation with large Q parameter value

This bulletin describes the immediate security measures to prevent the malicious exploitation of this vulnerability. We strongly recommend that users of the affected products apply these measures.

Rev A: CVE-2022-4304 is removed from the affected items as it affects only the server implementation that is not used in our products.

2. Affected products and components

Component	Product & Versions	Description
OpenSSL	PcVue 12 PcVue 15 PcVue 16	Use of a vulnerable version of the OpenSSL library

3. Impact

The 2 vulnerabilities referenced have various impacts:

- CVE-2023-4807: On Windows 64 platform running on x86_64 processors supporting the AVX512-IFMA instructions, an attacker could enforce the use of a vulnerable algorithm. It can then generate a fatal error in the application leading to a Denial of Service or enable the attacker to get complete control of the application process.
- CVE-2023-5678: Diffie-Hellman checks could lead to a Denial of Service when the parameters or the key are obtained from an untrusted source.

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.

4. Vulnerability details

4.1 POLY1305 MAC implementation corrupts XMM registers on Windows

CVE Id	CVE-2023-4807			
Publication date	2023-08-09			
Description	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions.			
Impact	The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000 The FIPS provider is not affected by this issue.			
CVSS v3.1 Base Score	7.8			
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H			
Attack Vector	Network	Adjacent	**Local**	Physical
Attack Complexity	**Low**		High	
Privileges Required	None	**Low**	High	
User interaction	**None**		Required	
Scope	Changed		**Unchanged**	
Confidentiality	**High**	Low	None	
Integrity	**High**	Low	None	
Availability	**High**	Low	None	
CWE Ids	*No CWE referenced*			

4.2 Excessive time spent in DH check / generation with large Q parameter value

CVE Id	CVE-2023-5678			
Publication date	2023-11-06			
Description	Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().			
Impact	An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack.			
CVSS v3.1 Base Score	5.3			
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L			
Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low		High	
Privileges Required	None	Low	High	
User interaction	None		Required	
Scope	Changed		Unchanged	
Confidentiality	High	Low	None	
Integrity	High	Low	None	
Availability	High	Low	None	
CWE Ids	CWE-754: Improper Check for Unusual or Exceptional Conditions			

5. Immediate risk mitigation

5.1 Harden the configuration

Who should apply this recommendation: All users
The system operators are highly recommended to take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- 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.
- Operate PcVue with a standard user. Administrative rights are only required at installation or for deployment purposes.

5.2 Update PcVue

Who should apply this recommendation: All users using the affected component
Apply the patch by installing a fixed PcVue version.

6. Available patches

Vulnerability	Product
CVE-2023-4807 – fixed in OpenSSL 3.1.3 & 3.2.0 CVE-2023-5678 – fixed in OpenSSL 3.1.5 & 3.2.0	Fixed in: • PcVue 16.1.2 – with OpenSSL 3.2.0 • PcVue 16.2.0 – with OpenSSL 3.2.1

7. Credits

N/A

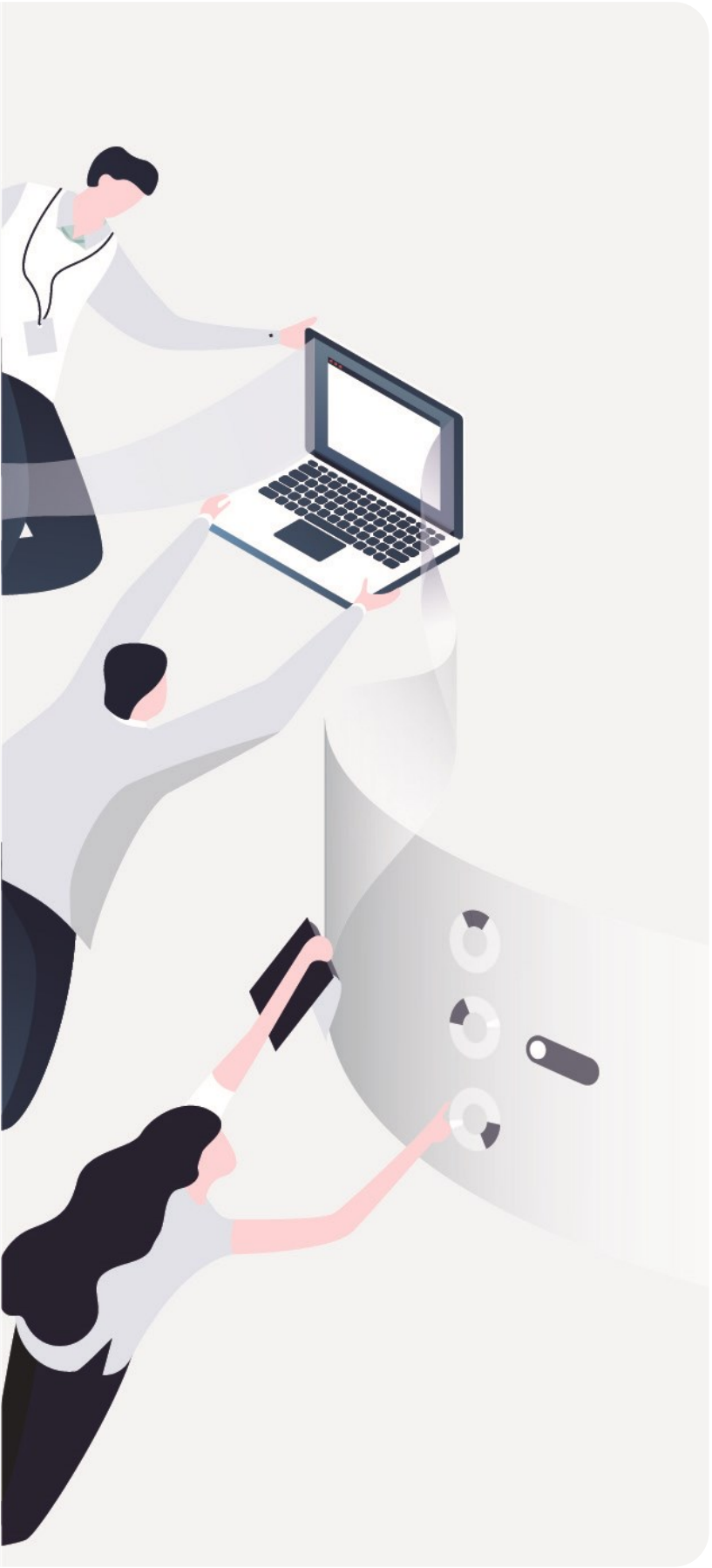
8. References

The public ARC Informatique security alert page: www.pcvuesolutions.com

CVE:

- CVE-2023-4807
- CVE-2023-5678

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



SECURITY BULLETIN

2023-3

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
2 avenue de la Cristallerie,
92310 Sèvres, France
Tél: +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