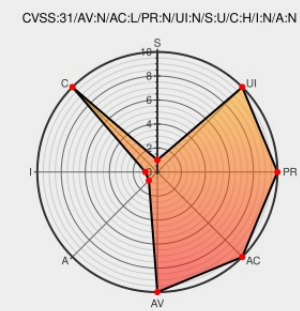
CVE-2023-24025

Published on: Not Yet Published

Last Modified on: 02/03/2023 03:00:00 PM UTC

CVE-2023-24025

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



Certain versions of Pqclean from Pqclean Project contain the following vulnerability:

CRYSTALS-DILITHIUM (in Post-Quantum Cryptography Selected Algorithms 2022) in PQClean d03da30 may allow universal forgeries of digital signatures via a template side-channel attack because of intermediate data leakage of one vector.

CVE-2023-24025 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Post-Quantum Cryptography | CSRC	csrc.nist.gov text/html	MISC csrc.nist.gov/Projects/post-quantum-cryptography/selected-algori 2022
GitHub - PQClean/PQClean at d03da3053491e767ef842deaef43fc5bdb6bc911	github.com text/html	MISC github.com/PQClean/PQClean/tree/d03da3053491e767ef842deaef43fc5b
A Practical Template Attack on CRYSTALS-Dilithium	eprint.iacr.org text/html	MISC eprint.iacr.org/2023/050

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pqclean Project	Pqclean	-	All	All	All

cpe:2.3:a:pqclean_project:pqclean:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-24025 : CRYSTALS-DILITHIUM in Post-Quantum Cryptography Selected Algorithms 2022 in PQClean d03da30 may… twitter.com/i/web/status/1…	2023-01-20 21:03:19
@threatmeter	CVE-2023-24025 CRYSTALS-DILITHIUM (in Post-Quantum Cryptography Selected Algorithms 2022) in PQClean d03da30 may al… twitter.com/i/web/status/1…	2023-01-21 04:09:45

← Previous ID

Next ID→