



CVE-2023-24025

Published on: Not Yet Published

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

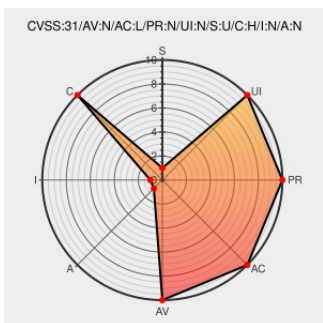
CVE-2023-24025

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 PQCclean 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 [M](#) 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-algorithms/2022
GitHub - PQCclean/PQCclean at d03da3053491e767ef842deaef43fc5bdb6bc911	github.com text/html	MISC github.com/PQCclean/PQCclean/tree/d03da3053491e767ef842deaef43fc5bdb6bc911
A Practical Template Attack on CRYSTALS-Dilithium	eprint.iacr.org text/html	MISC eprint.iacr.org/2023/050

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)