



CVE-2023-44378

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-44378
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-09 14:15:00 UTC
Updated	2023-10-13 18:43:00 UTC
Description	gnark is a zk-SNARK library that offers a high-level API to design circuits. Prior to version 0.9.0, for some in-circuit values, i

Risk And Classification

Problem Types: CWE-191

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Consensys	Gnark	All	All	All	All

References

Reference	Source	Link
LessThan(n) is unsafe with n = 254 · Issue #116 · zkopru-network/zkopru · GitHub	MISC	github.com
fix: assert that the binary decomposition of a variable is less than ... · Consensys/gnark@59a4087 · GitHub	MISC	github.com
Unsoundness in variable comparison / non-unique binary decomposition · Advisory · Consensys/gnark · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995500](#) GO (Go) Security Update for github.com/consensys/gnark (GHSA-498w-5j49-vqjg)

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](#).

Free CVE JSON API cve.report/api

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