



CVE-2021-21405

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

Summary

CVE	CVE-2021-21405
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-15 22:15:00 UTC
Updated	2021-04-23 14:40:00 UTC
Description	Lotus is an Implementation of the Filecoin protocol written in Go. BLS signature validation in lotus uses blst library method \

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Filecoin	Lotus	All	All	All	All

References

Reference	Source	Link
BLS Signature "Malleability" · Advisory · filecoin-project/lotus · GitHub	CONFIRM	github
A_DESCRIPTION.md · GitHub	MISC	github
refactor: switch to filecoin-ffi bls api for bls signatures by dignifiedquire · Pull Request #5393 · filecoin-project/lotus · GitHub	MISC	github
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982428](#) Go (go) Security Update for github.com/filecoin-project/lotus (GHSA-4g52-pqcj-phvh)

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