



CVE-2022-31111

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

Summary

CVE	CVE-2022-31111
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-06 18:15:00 UTC
Updated	2022-07-14 14:18:00 UTC
Description	Frontier is Substrate's Ethereum compatibility layer. In affected versions the truncation done when converting between EVM

Risk And Classification

Problem Types: CWE-670

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Parity	Frontier	-	All	All	All

References

Reference	Source
Limit number of iterations in genesis nonce building (#753) · paritytech/frontier@e3e427f · GitHub	MISC
Discrepancy between appeared EVM transfer value and actual value due to incorrect truncation · Advisory · paritytech/frontier · GitHub	CONFIRMED
Limit number of iterations in genesis nonce building (#753) · paritytech/frontier@fed5e0a · GitHub	MISC
Fix incorrect truncation of low_u128/low_u64 by sorpaas · Pull Request #753 · paritytech/frontier · GitHub	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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