



CVE-2023-28431

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

Summary

CVE	CVE-2023-28431
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-22 21:15:00 UTC
Updated	2023-11-07 04:10:00 UTC
Description	Frontier is an Ethereum compatibility layer for Substrate. Frontier's `modexp` precompile uses `num-bigint` crate under the

Risk And Classification

Problem Types: CWE-682

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
modexp precompile is slow for even modulus · Advisory · paritytech/frontier · GitHub	MISC	github.com	
Increase modexp gas cost when mod is even by sorpaas · Pull Request #1017 · paritytech/frontier · GitHub	MISC	github.com	
Increase modexp gas cost when mod is even (#1017) · paritytech/frontier@5af12e9 · GitHub	MISC	github.com	
num-bigint/power.rs at 6f2b8e0fc218dbd0f49bebb8db2d1a771fe6bafa · rust-num/num-bigint · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

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