CVE-2019-20399

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-20399
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-23 00:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	A timing vulnerability in the Scalar::check_overflow function in Parity libsecp256k1-rs before 0.3.1 potentially allows an attac

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Parity	Libsecp256k1	All	All	All	All
Application	Parity	Libsecp256k1	All	All	All	All

References

Reference	Source	Link	Tags
Prevent side channel leak in Scala::check_overflow · paritytech/libsecp256k1@11ba23a · GitHub	MISC	github.com	Patch, Third
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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