CVE-2021-38195

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

Summary

CVE	CVE-2021-38195
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-08 06:15:00 UTC
Updated	2021-08-16 16:51:00 UTC
Description	An issue was discovered in the libsecp256k1 crate before 0.5.0 for Rust. It can verify an invalid signature because it allows

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
raw.githubusercontent.com/rustsec/advisory-db/main/crates/libsecp256k1/RUSTSEC-2021-007...	MISC	raw.githubuse
RUSTSEC-2021-0076: libsecp256k1: libsecp256k1 allows overflowing signatures › RustSec Advisory Database	MISC	rustsec.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**