



CVE-2021-45696

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

Summary

CVE	CVE-2021-45696
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-27 00:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	An issue was discovered in the sha2 crate 0.9.7 before 0.9.8 for Rust. Hashes of long messages may be incorrect when the

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sha2 Project	Sha2	0.9.7	All	All	All

References

Reference	Source	Link
raw.githubusercontent.com/rustsec/advisory-db/main/crates/sha2/RUSTSEC-2021-0100.md	MISC	raw.githubusercontent.com/rustsec/advisory-db/main/crates/sha2/RUSTSEC-2021-0100.md
RUSTSEC-2021-0100: sha2: Miscomputed results when using AVX2 backend › 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.

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