CVE-2021-43571

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

Summary

CVE	CVE-2021-43571
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-09 22:15:00 UTC
Updated	2021-11-12 19:59:00 UTC
Description	The verify function in the Stark Bank Node.js ECDSA library (ecdsa-node) 1.1.2 fails to check that the signature is non-zero

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Starkbank	Ecdsa-node	1.1.2	All	All	All

References

Reference
Technical Advisory – Arbitrary Signature Forgery in Stark Bank ECDSA Libraries (CVE-2021-43572, CVE-2021-43570, CVE-2021-43569, CVI
Release v1.1.3 · starkbank/ecdsa-node · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980155 Nodejs (npm) Security Update for starkbank-ecdsa (GHSA-q9q6-f556-gpm7)

Free CVE JSON API cve.report/api

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