



CVE-2021-43570

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

Summary

CVE	CVE-2021-43570
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 19:58:00 UTC
Description	The verify function in the Stark Bank Java ECDSA library (ecdsa-java) 1.0.0 fails to check that the signature is non-zero, wr

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Starkbank	Ecdsa-java	1.0.0	All	All	All

References

Reference

Release v1.0.1 · starkbank/ecdsa-java · GitHub
Technical Advisory – Arbitrary Signature Forgery in Stark Bank ECDSA Libraries (CVE-2021-43572, CVE-2021-43570, CVE-2021-43569, CVI
CVE Program record
NVD vulnerability detail

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