



CVE-2021-43572

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

Summary

CVE	CVE-2021-43572
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-09 22:15:00 UTC
Updated	2022-03-24 15:57:00 UTC
Description	The verify function in the Stark Bank Python ECDSA library (aka starkbank-escada or ecdsa-python) before 2.0.1 fails to ch

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Starkbank	Ecdsa-python	All	All	All	All
Application	Starkbank	Ecdsa-python	2.0.0	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 v2.0.1 · starkbank/ecdsa-python · GitHub
Add signature.r and signature.s range check · starkbank/ecdsa-python@d136170 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980154](#) Python (pip) Security Update for starkbank-ecdsa (GHSA-92vm-mxjf-jqf3)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)