CVE-2021-21241

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

Summary

CVE	CVE-2021-21241
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-11 21:15:00 UTC
Updated	2021-01-19 15:43:00 UTC
Description	The Python "Flask-Security-Too" package is used for adding security features to your Flask application. It is an is a indeper

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flask-security-too Project	Flask-security-too	All	All	All	All
Application	Flask-security-too Project	Flask-security-too	All	All	All	All

References

Reference
Fix security vuln - GET on /login or /change could reveal authenticat… · Flask-Middleware/flask-security@6d50ee9 · GitHub
Flask-Security-Too · PyPI
Release Fix CSRF Vulnerability · Flask-Middleware/flask-security · GitHub
CSRF Vuln can expose users authentication token · Advisory · Flask-Middleware/flask-security · GitHub
Fix security vuln - GET on /login or /change could reveal authenticat… by jwag956 · Pull Request #422 · Flask-Middleware/flask-security · GitH
I421backport (#425) · Flask-Middleware/flask-security@61d3131 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179957 Debian Security Update for flask-security (CVE-2021-21241)

752549 SUSE Enterprise Linux Security Update for python-Flask-Security-Too (SUSE-SU-2022:3093-1)

983060 Python (pip) Security Update for Flask-Security-Too (GHSA-hh7m-rx4f-4vpv)

Free CVE JSON API cve.report/api

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