



CVE-2022-24880

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

Summary

CVE	CVE-2022-24880
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-25 22:15:00 UTC
Updated	2022-05-05 18:20:00 UTC
Description	flask-session-captcha is a package which allows users to extend Flask by adding an image based captcha stored in a serve

Risk And Classification

Problem Types: CWE-754

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flask-session-captcha Project	Flask-session-captcha	All	All	All	All

References

Reference	Source
Release v1.2.1 · Tethik/flask-session-captcha · GitHub	MITRE
Potential Captcha Validate Bypass due to unexpected return value of validate-function · Advisory · Tethik/flask-session-captcha · GitHub	CC
add some extra tests to ensure False is returned · Tethik/flask-session-captcha@2811ae2 · GitHub	MITRE
Fix `validate()` returned value by GuillaumeGomez · Pull Request #27 · Tethik/flask-session-captcha · GitHub	MITRE
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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