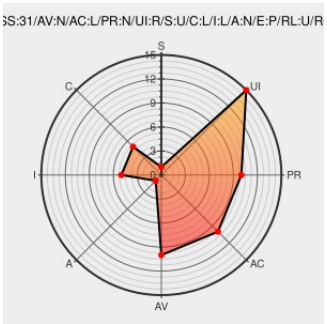
CVE-2021-23385

Published on: Not Yet Published

Last Modified on: 08/28/2023 07:15:00 PM UTC

CVE-2021-23385

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Flask-security from Flask-security Project contain the following vulnerability:

This affects all versions of package Flask-Security. When using the get_post_logout_redirect and get_post_login_redirect functions, it is possible to bypass URL validation and redirect a user to an arbitrary URL by providing multiple back slashes such as \\\evil.com/path. This vulnerability is only exploitable if an alternative WSGI server other than Werkzeug is used, or the default behaviour of Werkzeug is modified using 'autocorrect_location_header=False. **Note:** Flask-Security is not maintained anymore.

CVE-2021-23385 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
GitHub - mattupstate/flask-security: Quick and simple security for Flask applications	github.com text/html	MISC github.com/mattupstate/flask-security
[SECURITY] [DLA 3545-1] flask-security security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230828 [SECURITY] [DLA 3545-1] flask-security security update
Open Redirect in flask-security | CVE-2021-23385 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-PYTHON-FLASKSECURITY-1293234
URL confusion vulnerabilities in the wild: Exploring parser inconsistencies | Snyk	snyk.io text/html	MISC snyk.io/blog/url-confusion-vulnerabilities/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

181894 Debian Security Update for flask-security (CVE-2021-23385)

376262 Python Flask-Security Plugin Open Redirect Vulnerability

6000087 Debian Security Update for flask-security (DLA 3545-1)

752761 SUSE Enterprise Linux Security Update for python-Flask-Security-Too (SUSE-SU-2022:3867-1)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:flask-security_project:flask-security:*:*:*:*:*:*:*:*:

Discovery Credit

Noam Moshe of Claroty

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23385 : This affects all versions of package Flask-Security. When using the get_post_logout_redirect and… twitter.com/i/web/status/1…	2022-08-02 13:37:15
@LinInfoSec	Python - CVE-2021-23385: security.snyk.io/vuln/SNYK-PYTH…	2022-08-02 17:00:19
@4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #Analysed #breach #vulnerability : CVE-2021-23385 (flask-security)	2022-08-12 06:07:04
/r/netcve	CVE-2021-23385	2022-08-02 14:39:47

← Previous ID

Next ID→

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