



CVE-2021-23401

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

Summary

CVE	CVE-2021-23401
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-05 11:15:00 UTC
Updated	2021-07-08 18:08:00 UTC
Description	This affects all versions of package Flask-User. When using the make_safe_url function, it is possible to bypass URL validation.

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
GitHub - lingthio/Flask-User: Customizable User Authorization & User Management: Register, Confirm, Login, Change username/password, F
Open Redirect in flask-user Snyk
Flask-User/user_manager__utils.py at master · lingthio/Flask-User · GitHub
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit
LEGACY: Noam Moshe of Claroty

Legacy QID Mappings

376251 Python Flask-User Plugin Open Redirect Vulnerability

© [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](#)