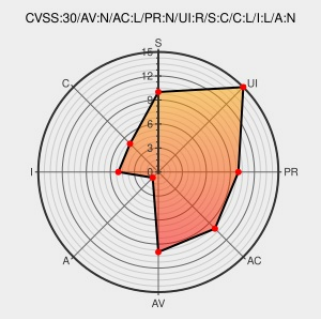
CVE-2018-16516

Published on: 09/05/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:53:00 AM UTC

CVE-2018-16516

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



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

helpers.py in Flask-Admin 1.5.2 has Reflected XSS via a crafted URL.

CVE-2018-16516 has been assigned by cve@mitre.org 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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[SECURITY] Fedora 32 Update: python-flask-admin-1.5.6-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-e8f384af5f
[SECURITY] Fedora 31 Update: python-flask-admin-1.5.6-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-4aaf6e6d7c

refs #1503 fix reflected xss by lbhsot · Pull Request #1699 · flask-admin/flask-admin · GitHub	Exploit Vendor Advisory github.com text/html	MISC github.com/flask-admin/flask-admin/pull/1699

Related QID Numbers

981208 Python (pip) Security Update for flask-admin (GHSA-894g-6j7q-2hx6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flask-admin Project	Flask-admin	1.5.2	All	All	All
Application	Flask-admin Project	Flask-admin	1.5.2	All	All	All

cpe:2.3:a:flask-admin_project:flask-admin:1.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:flask-admin_project:flask-admin:1.5.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→