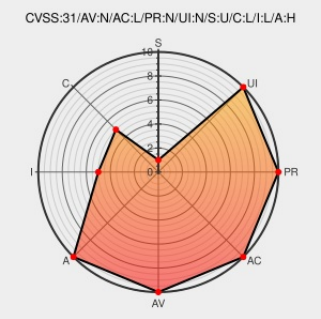
CVE-2022-30034

Published on: Not Yet Published

Last Modified on: 10/26/2022 10:48:00 PM UTC

CVE-2022-30034

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



Certain versions of Flower from Flower Project contain the following vulnerability:

Flower, a web UI for the Celery Python RPC framework, all versions as of 05-02-2022 is vulnerable to an OAuth authentication bypass. An attacker could then access the Flower API to discover and invoke arbitrary Celery RPC calls or deny service by shutting down Celery task nodes.

CVE-2022-30034 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.6 - HIGH

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
No Description Provided	githubcommherflower.com Inactive Link Not Archived	MISC githubcommherflower.com

Multiple Vulnerabilities in Flower and Downstream Attacks on Airflow | Tanner Prynn	tprynn.github.io text/html	MISC tprynn.github.io/2022/05/26/flower-vulns.html
Security Vulnerabilities in Flower: OAuth Authentication Bypass and Lack of CSRF Protections (CVE-2022-30034) · Issue #1217 · mher/flower · GitHub	github.com text/html	MISC github.com/mher/flower/issues/1217

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flower Project	Flower	All	All	All	All
Application	Flower Project	Flower	All	All	All	All

cpe:2.3:a:flower_project:flower:*:*:*:*:*:*:*:*:

cpe:2.3:a:flower_project:flower:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@tannerprynn	Multiple vulnerabilities in Flower (CVE-2022-30034) and downstream attacks on Apache Airflow tprynn.github.io/2022/05/26/flo…	2022-05-26 17:31:11
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-30034 Flower, a web UI for the Celery Python RPC framework, all version… twitter.com/i/web/status/1…	2022-05-31 15:55:56
@RedPacketSec	Flower security bypass | CVE-2022-30034 - redpacketsecurity.com/flower-securit…	2022-06-01 09:01:30
@CVEreport	CVE-2022-30034 : Flower, a web UI for the Celery Python RPC framework, all versions as of 05-02-2022 is vulnerable… twitter.com/i/web/status/1…	2022-06-02 14:06:05
/r/netcve	CVE-2022-30034	2022-06-02 14:38:49

← Previous ID

Next ID→

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