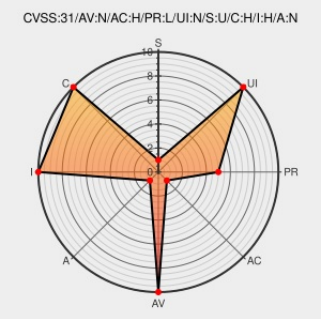
CVE-2021-43777

Published on: Not Yet Published

Last Modified on: 11/30/2021 03:39:00 PM UTC

CVE-2021-43777 - advisory for GHSA-vhc7-w7r8-8m34

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Redash from Redash contain the following vulnerability:

Redash is a package for data visualization and sharing. In Redash version 10.0 and prior, the implementation of Google Login (via OAuth) incorrectly uses the `state` parameter to pass the next URL to redirect the user to after login. The `state` parameter should be used for a Cross-Site Request Forgery (CSRF) token, not a static and easily predicted value. This vulnerability does not affect users who do not use Google Login for their instance of Redash. A patch in the `master` and `release/10.x.x` branches addresses this by replacing `Flask-Oauthlib` with `Authlib` which automatically provides and validates a CSRF token for the state variable. The new implementation stores the next URL on the user session object. As a workaround, one may disable Google Login to mitigate the vulnerability.

CVE-2021-43777 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **getredash** - **redash** version **<= 10.0**

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: 5.8 - MEDIUM

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

PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Insecure use of state parameter for Google OAuth Login · Advisory · getredash/redash · GitHub	github.com text/html	CONFIRM github.com/getredash/redash/security/advisories/GHSA-vhc7-w7r8-8m34
Merge pull request from GHSA-vhc7-w7r8-8m34 · getredash/redash@da696ff · GitHub	github.com text/html	MISC github.com/getredash/redash/commit/da696ff7f84787cbf85967460fac52886cbe063e

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redash	Redash	All	All	All	All

cpe:2.3:a:redash:redash:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@SecRiskRptSME	RT: CVE-2021-43777 Redash is a package for data visualization and sharing. In Redash version 10.0 and prior, the i… twitter.com/i/web/status/1…	2021-11-24 08:33:55
@CVEreport	CVE-2021-43777 : Redash is a package for data visualization and sharing. In Redash version 10.0 and prior, the impl… twitter.com/i/web/status/1…	2021-11-24 15:17:53

← Previous ID

Next ID→