



# CVE-2021-43777

Published on: Not Yet Published

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

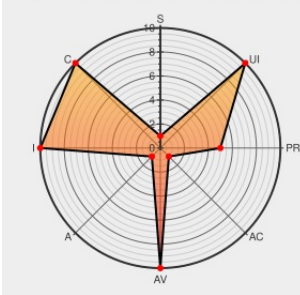
## CVE-2021-43777 - advisory for GHSA-vhc7-w7r8-8m34

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N



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.

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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
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	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/getredash/redash/security/advisories/GHSA-vhc7-w7r8-8m34">github.com/getredash/redash/security/advisories/GHSA-vhc7-w7r8-8m34</a>
Merge pull request from GHSA-vhc7-w7r8-8m34 · getredash/redash@da696ff · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/getredash/redash/commit/da696ff7f84787cbf85967460fac52886cbe063e">github.com/getredash/redash/commit/da696ff7f84787cbf85967460fac52886cbe063e</a>

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](mailto: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	Redash	Redash	All	All	All	All
<code>cpe:2.3:a:redash:redash:*****:</code>						

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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-11-24 15:17:53

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022 |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)