

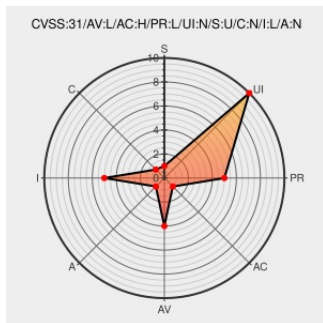


CVE-2022-31072

Published on: Not Yet Published

Last Modified on: 06/27/2022 06:20:00 PM UTC

CVE-2022-31072 - advisory for GHSA-g28x-pgr3-qqx6

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Octokit](#) from [Octokit Project](#) contain the following vulnerability:

Octokit is a Ruby toolkit for the GitHub API. Versions 4.23.0 and 4.24.0 of the octokit gem were published containing world-writable files. Specifically, the gem was packed with files having their permissions set to `-rw-rw-rw-` (i.e. 0666) instead of `-rw-r--r--` (i.e. 0644). This means everyone who is not the owner (Group and Public) with access to the

instance where this release had been installed could modify the world-writable files from this gem. This issue is patched in Octokit 4.25.0. Two workarounds are available. Users can use the previous version of the gem, v4.22.0. Alternatively, users can modify the file permissions manually until they are able to upgrade to the latest version.

CVE-2022-31072 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: [octokit](#) - `octokit.rb` version `>= 4.23.0, < 4.25.0`

CVSS3 Score: **3.3 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Octokit gem published with world-writable files · Advisory · octokit/octokit.rb · GitHub	github.com text/html	 CONFIRM github.com/octokit/octokit.rb/security/advisories/GHSA-g28x-pgr3-qqx6
Merge pull request #1446 from octokit/updates-release-steps-ic · octokit/octokit.rb@1c8edec · GitHub	github.com text/html	 MISC github.com/octokit/octokit.rb/commit/1c8edec9cf23d1ceb959d91a416a69f55ce7d55

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	Octokit Project	Octokit	4.23.0	All	All	All
Application	Octokit Project	Octokit	4.24.0	All	All	All
cpe:2.3:a:octokit_project:octokit:4.23.0:*:*:*:ruby:*:*						
cpe:2.3:a:octokit_project:octokit:4.24.0:*:*:*:ruby:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-31072 : Octokit is a Ruby toolkit for the GitHub API. Versions 4.23.0 and 4.24.0 of the octokit gem were p... twitter.com/i/web/status/1...	2022-06-15 22:39:43
 @LinInfoSec	Ruby - CVE-2022-31072: github.com/octokit/octoki...	2022-06-16 01:00:23
 @RemotelyAlerts	Severity: ? Octokit is a Ruby toolkit for the GitHub... CVE-2022-31072 Link for more: alerts.remotelymmm.com/CVE-2022-31072	2022-06-27 19:33:16
 /r/netcve	CVE-2022-31072	2022-06-15 23:38:51

[← Previous ID](#)

[Next ID →](#)

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](#)