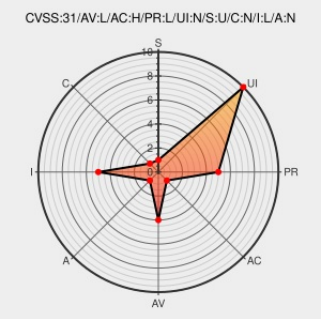
CVE-2022-31071

Published on: Not Yet Published

Last Modified on: 06/27/2022 06:17:00 PM UTC

CVE-2022-31071 - advisory for GHSA-26qj-cr27-r5c4

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



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

Octopoller is a micro gem for polling and retrying. Version 0.2.0 of the octopoller gem was published containing world-writeable 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 Octopoller 0.3.0. Two workarounds are available. Users can use the previous version of the gem, v0.1.0. Alternatively, users can modify the file permissions manually until they are able to upgrade to the latest version.

CVE-2022-31071 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **octokit** - **octopoller.rb** version **= 0.2.0**

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
Merge pull request #25 from octokit/updates-release-steps-checks · octokit/octopoller.rb@abed2b8 · GitHub	github.com text/html	MISC github.com/octokit/octopoller.rb/commit/abed2b8d05abe2cc3eb6bdfb34e53d465e7c7874
Octopoller gem published with world-writable files · Advisory · octokit/octopoller.rb · GitHub	github.com text/html	CONFIRM github.com/octokit/octopoller.rb/security/advisories/GHSA-26qj-cr27-r5c4

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Octopoller Project	Octopoller	0.2.0	All	All	All

cpe:2.3:a:octopoller_project:octopoller:0.2.0:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31071 : Octopoller is a micro gem for polling and retrying. Version 0.2.0 of the octopoller gem was publis… twitter.com/i/web/status/1…	2022-06-15 22:44:12
@RemotelyAlerts	Severity: ? | Octopoller is a micro gem for polling an... | CVE-2022-31071 | Link for more: alerts.remotelyrmm.com/CVE-2022-31071	2022-06-27 19:35:04
/r/netcve	CVE-2022-31071	2022-06-15 23:38:52

← Previous ID

Next ID→