

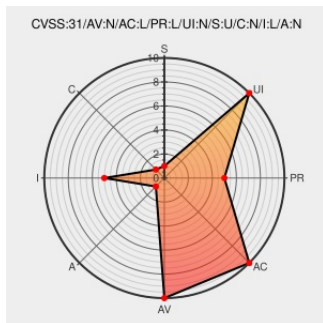


# CVE-2022-1502

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

## CVE-2022-1502

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

Certain versions of [Server](#) from [Octopus](#) contain the following vulnerability:

Permissions were not properly verified in the API on projects using version control in Git. This allowed projects to be modified by users with only ProjectView permissions.

CVE-2022-1502 has been assigned by [security@octopus.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Octopus Deploy](#) - **Octopus Server** version **2022.1.2454** <

Affected Vendor/Software: [Octopus Deploy](#) - **Octopus Server** version **2021.3.12725** <

CVSS3 Score: **4.3 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **3.5 - LOW**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

Security Advisory 2022-03 | Octopus Deploy Security Advisories

advisories.octopus.com

text/html

MISC

advisories.octopus.com/post/2022/sa2022-03/

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                     | Octopus | Server  | All     | All    | All     | All      |
| cpe:2.3:a:octopus:server:*****: |         |         |         |        |         |          |

No vendor comments have been submitted for this CVE

Social Mentions

| Source     | Title                                                                                                                                                                                                    | Posted (UTC)        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| @CVEreport | CVE-2022-1502 : Permissions were not properly verified in the API on projects using version control in Git. This al... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-05-04 06:19:56 |
| /r/netcve  | <a href="#">CVE-2022-1502</a>                                                                                                                                                                            | 2022-05-04 07:38:36 |

← Previous ID

Next ID →