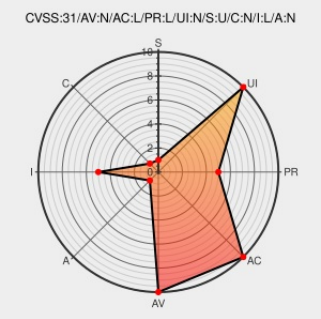
CVE-2022-1502

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
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: 3.5 - LOW

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

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/

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… twitter.com/i/web/status/1…	2022-05-04 06:19:56
/r/netcve	CVE-2022-1502	2022-05-04 07:38:36

← Previous ID

Next ID→