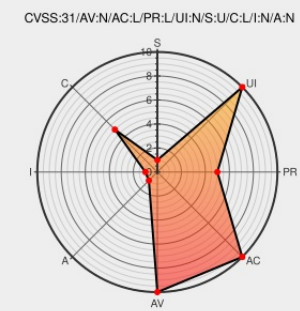
CVE-2021-31818

Published on: 06/17/2021 12:00:00 AM UTC

Last Modified on: 07/27/2022 05:20:00 PM UTC

CVE-2021-31818

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



Certain versions of Server from Octopus contain the following vulnerability:

Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API because user supplied data in the API request isn't parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables.

CVE-2021-31818 has been assigned by security@octopus.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Octopus Deploy** - **Octopus Server** version **>= 2018.9.17**

Affected Vendor/Software: **Octopus Deploy** - **Octopus Server** version **< 2020.6.5146**

Affected Vendor/Software: **Octopus Deploy** - **Octopus Server** version **>= 2021.1.7149**

Affected Vendor/Software: **Octopus Deploy** - **Octopus Server** version **< 2021.1.7316**

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	LOW	NONE	NONE

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
2021-04 - SQL Injection in the Events REST API (CVE-2021-31818)	advisories.octopus.com text/html	MISC advisories.octopus.com/adv/2021-04---SQL-Injection-in-the-Events-REST-API-(CVE-2021-31818).2013233248.html

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-2021-31818 : Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in t… twitter.com/i/web/status/1…	2021-06-17 13:30:33
/r/netcve	CVE-2021-31818	2021-06-17 14:41:12

← Previous ID

Next ID→