CVE-2020-27155

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-27155
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-22 17:15:00 UTC
Updated	2020-10-30 14:08:00 UTC
Description	An issue was discovered in Octopus Deploy through 2020.4.4. If enabled, the websocket endpoint may allow an untrusted t

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Octopus	Octopus Deploy	All	All	All	All

References

Reference	Source	Link	T
WebSocket polling endpoint can allow untrusted connections · Issue #6637 · OctopusDeploy/Issues · GitHub	MISC	github.com	Is
Octopus Deploy · GitHub	MISC	github.com	T
WebSocket polling endpoint can allow untrusted connections · Issue #6640 · OctopusDeploy/Issues · GitHub	MISC	github.com	Is
WebSocket polling endpoint can allow untrusted connections · Issue #6639 · OctopusDeploy/Issues · GitHub	MISC	github.com	Is
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report