



CVE-2022-23652

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-23652
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-22 20:15:00 UTC
Updated	2022-03-01 20:08:00 UTC
Description	capsule-proxy is a reverse proxy for Capsule Operator which provides multi-tenancy in Kubernetes. In versions prior to 0.2.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clastix	Capsule-proxy	All	All	All	All

References

Reference	Source	Link
Privilege escalation vulnerability via malicious "Connection" header · Issue #188 · clastix/capsule-proxy · GitHub	MISC	github.com
bug: cve exploiting malicious connection header · clastix/capsule-proxy@efe91f6 · GitHub	MISC	github.com
Privilege escalation using hop-by-hop Connection header · Advisory · clastix/capsule-proxy · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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