



CVE-2021-25743

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-25743
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-07 00:15:00 UTC
Updated	2022-02-28 15:22:00 UTC
Description	kubectl does not neutralize escape, meta or control sequences contained in the raw data it outputs to a terminal. This includ

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	All	All	All	All

References

Reference	Source	Link
ANSI escape characters in kubectl output are not being filtered · Issue #101695 · kubernetes/kubernetes · GitHub	CONFIRM	github.com
CVE-2021-25743 Kubernetes Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.neta
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Eviatar Gerzi

Legacy QID Mappings

284120 Fedora Security Update for kubernetes (FEDORA-2023-a1d7a29fe5)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)