



CVE-2021-25740

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

Summary

CVE	CVE-2021-25740
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-20 17:15:00 UTC
Updated	2021-11-06 02:49:00 UTC
Description	A security issue was discovered with Kubernetes that could enable users to send network traffic to locations they would oth

Risk And Classification

Problem Types: CWE-610

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- [Security Advisory] CVE-2021-25740: Endpoint & EndpointSlice permissions allow cross-Namespace forwarding
- CVE-2021-25740: Endpoint & EndpointSlice permissions allow cross-Namespace forwarding · Issue #103675 · kubernetes/kubernetes · GitHub
- CVE-2021-25740 Kubernetes Vulnerability in NetApp Products | NetApp Product Security
- CVE Program record
- NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Rob Scott

Legacy QID Mappings

180887 Debian Security Update for kubernetes (CVE-2021-25740)

© [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](#)