



CVE-2021-25737

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

Summary

CVE	CVE-2021-25737
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-06 12:15:00 UTC
Updated	2021-10-07 17:55:00 UTC
Description	A security issue was discovered in Kubernetes where a user may be able to redirect pod traffic to private networks on a No

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.21.0	-	All	All

References

Reference	Source
CVE-2021-25737 Kubernetes Vulnerability in NetApp Products NetApp Product Security	CONFID
[Security Advisory] CVE-2021-25737: Holes in EndpointSlice Validation Enable Host Network Hijack	MISC
CVE-2021-25737: Holes in EndpointSlice Validation Enable Host Network Hijack · Issue #102106 · kubernetes/kubernetes · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: John Howard

Legacy QID Mappings

[180886](#) Debian Security Update for kubernetes (CVE-2021-25737)

239525 Red Hat Update for OpenShift Container Platform 4.8.2 (RHSA-2021:2437)
376958 Kubernetes kube-Apiserver EndpointSlice Validation Vulnerability
770074 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:2437)
770111 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-2437)
980534 Go (go) Security Update for k8s.io/kubernetes (GHSA-mfv7-gq43-w965)

© [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](#)