



CVE-2021-25736

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

Summary

CVE	CVE-2021-25736
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-30 03:15:00 UTC
Updated	2023-12-21 22:15:00 UTC
Description	Kube-proxy on Windows can unintentionally forward traffic to local processes listening on the same port ("spec.ports[*].port"

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference

- [CVE-2021-25736 Kubernetes Vulnerability in NetApp Products | NetApp Product Security](#)
- [For LoadBalancer Service type don't create a HNS policy for empty or invalid external loadbalancer IP by sbangari · Pull Request #99958 · kubernetes/kubernetes](#)
- [\[Security Advisory\] CVE-2021-25736: Windows kube-proxy LoadBalancer contention](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995790](#) GO (Go) Security Update for k8s.io/kubernetes (GHSA-35c7-w35f-xwgh)

© [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](#)