



CVE-2021-25745

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

Summary

CVE	CVE-2021-25745
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-06 01:15:00 UTC
Updated	2022-12-02 22:41:00 UTC
Description	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use the spec.r

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
[Security Advisory] CVE-2021-25745: Ingress-nginx `path` can be pointed to service account token file	MISC
CVE-2021-25745: Ingress-nginx `path` can be pointed to service account token file · Issue #8502 · kubernetes/ingress-nginx · GitHub	MISC
May 2022 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	CONFIRMED
CVE Program record	CVE PROGRAM
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Gafnit Amiga

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

© [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](#)