CVE-2023-3676

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-3676
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-31 21:15:00 UTC
Updated	2023-11-30 22:15:00 UTC
Description	A security issue was discovered in Kubernetes where a user that can create pods on Windows nodes may be able to escala

Risk And Classification

Problem Types: CWE-20

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-2023-3676: Insufficient input sanitization on Windows nodes leads to privilege escalation · Issue #119339 · kubernetes/kubernetes · GitH
security.netapp.com/advisory/ntap-20231130-0007
[Security Advisory] CVE-2023-3676: Insufficient input sanitization on Windows nodes leads to privilege escalation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

285293 Fedora Security Update for kubernetes (FEDORA-2023-8f8ddb2428)

995890 GO (Go) Security Update for k8s.io/kubernetes (GHSA-7fxm-f474-hf8w)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report