CVE-2023-3893

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

Summary

CVE	CVE-2023-3893
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 18:15:00 UTC
Updated	2023-11-14 18:00:00 UTC
Description	A security issue was discovered in Kubernetes where a user that can create pods on Windows nodes running kubernetes-c

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Csi Proxy	2.0.0	alpha0	All	All
Application	Kubernetes	Csi Proxy	All	All	All	All

References

Reference
CVE-2023-3893: Insufficient input sanitization on kubernetes-csi-proxy leads to privilege escalation · Issue #119594 · kubernetes/kubernetes ·
[Security Advisory] CVE-2023-3893: Insufficient input sanitization on kubernetes-csi-proxy leads to privilege escalation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995827 GO (Go) Security Update for github.com/kubernetes-csi/csi-proxy (GHSA-r6cc-7wj7-gfx2)

Free CVE JSON API cve.report/api

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