



# CVE-2023-3893

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-3893
<b>State</b>	PUBLIC
<b>Assigner</b>	security@kubernetes.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-03 18:15:00 UTC
<b>Updated</b>	2023-11-14 18:00:00 UTC
<b>Description</b>	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	<a href="#">Kubernetes</a>	<a href="#">Csi Proxy</a>	2.0.0	alpha0	All	All
Application	<a href="#">Kubernetes</a>	<a href="#">Csi Proxy</a>	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)

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)