



CVE-2023-3676

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

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 escalate

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 · GitHub](#)
- [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)

© [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](#).

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

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