



CVE-2023-48713

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-48713
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-28 04:15:00 UTC
Updated	2023-12-01 21:53:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Knative	Serving	All	All	All	All

References

Reference	Source	Link	Tags
Bound buffer for reading stats (#14542) · knative/serving@012ee25 · GitHub		github.com	
Attacker-controlled pod can cause denial of service of autoscaler · Advisory · knative/serving · GitHub		github.com	
github.com/knative/serving/commit/fff40ef7bac9be8380ec3d1c70fc15b57093382a		github.com	
github.com/knative/serving/commit/101f814112b9ca0767f457e7e616b46205551cf1		github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[996070](#) GO (Go) Security Update for knative.dev/serving (GHSA-qmvj-4qr9-v547)

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