



CVE-2023-47090

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

Summary

CVE	CVE-2023-47090
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-30 17:15:00 UTC
Updated	2023-11-08 00:15:00 UTC
Description	NATS nats-server before 2.9.23 and 2.10.x before 2.10.2 has an authentication bypass. An implicit \$G user in an authoriza

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Nats-server	All	All	All	All

References

Reference	Source	Link	T
oss-security - Re: NATS: 2023-01: Adding accounts for just the system account adds auth bypass	MLIST	www.openwall.com	
Adding accounts for just the system account adds auth bypass · Advisory · nats-io/nats-server · GitHub	MISC	github.com	
oss-security - NATS: 2023-01: Adding accounts for just the system account adds auth bypass	MISC	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[907728](#) Common Base Linux Mariner (CBL-Mariner) Security Update for telegraf (31779-1)

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](#)