xkeys Seal encryption used fixed key for all encryption

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-46129
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-31 00:15:09 UTC
Updated	2026-03-30 14:30:00 UTC
Description	NATS.io is a high performance open source pub-sub distributed communication technology, built for the cloud, on-premise,

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-321 | CWE-325 | CWE-321 CWE-321: Use of Hard-coded Cryptographic Key | CWE-325 CWE-325: Missing Cryptographic Step

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Nats-io	Nkeys	affected >= 2.10.0, < 2.10.4	Not specified
CNA	Nats-io	Nkeys	affected >= 0.4.0, < 0.4.6	Not specified

References

Reference	Source	L
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	af854a3a-2127-422b-91ae-364da2661108	li
oss-security - NATS: 2023-02: nkeys: xkeys Seal encryption used fixed key for all encryption	af854a3a-2127-422b-91ae-364da2661108	w
xkeys Seal encryption used fixed key for all encryption · Advisory · nats-io/nkeys · GitHub	af854a3a-2127-422b-91ae-364da2661108	g
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	af854a3a-2127-422b-91ae-364da2661108	li
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

284776 Fedora Security Update for golang (FEDORA-2023-66966ae3d0)

285137 Fedora Security Update for golang (FEDORA-2023-3a895ff65c)

506120 Alpine Linux Security Update for nats-server

907623 Common Base Linux Mariner (CBL-Mariner) Security Update for telegraf (31792-1)

995792 GO (Go) Security Update for github.com/nats-io/nats-server/v2 (GHSA-mr45-rx8q-wcm9)

© 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 registred 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.

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