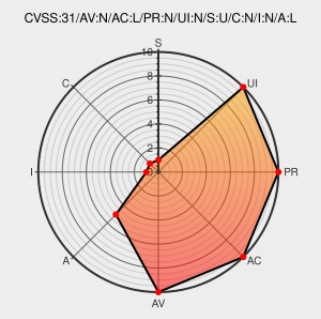
CVE-2023-33199

Published on: Not Yet Published

Last Modified on: 06/05/2023 02:21:00 PM UTC

CVE-2023-33199 - advisory for GHSA-frqx-jfcm-6jjr

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Rekor from Linuxfoundation contain the following vulnerability:

Rekor's goals are to provide an immutable tamper resistant ledger of metadata generated within a software projects supply chain. A malformed proposed entry of the `intoto/v0.0.2` type can cause a panic on a thread within the Rekor process. The thread is recovered so the client receives a 500 error message and service still continues, so the availability impact of this is minimal. This has been fixed in v1.2.0 of Rekor. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVE-2023-33199 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **sigstore** - **rekor** version **= < 1.2.0**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	LOW

CVE References

Description	Tags	Link
malformed proposed intoto v0.0.2 entries can cause a panic · Advisory · sigstore/rekor · GitHub	github.com text/html	MISC github.com/sigstore/rekor/security/advisories/GHSA-frqx-jfcm-6jjr
Merge pull request from GHSA-frqx-jfcm-6jjr · sigstore/rekor@140c5ad · GitHub	github.com text/html	MISC github.com/sigstore/rekor/commit/140c5add105179e5ffd9e3e114fd1b6b93aebbd4

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

907420 Common Base Linux Mariner (CBL-Mariner) Security Update for skopeo (26947-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Rekor	All	All	All	All

cpe:2.3:a:linuxfoundation:rekor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→