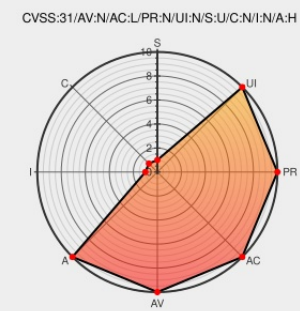
CVE-2023-25656

Published on: Not Yet Published

Last Modified on: 03/01/2023 06:31:00 PM UTC

CVE-2023-25656 - advisory for GHSA-87x9-7grx-m28v

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



Certain versions of Notation-go from Notation-go Project contain the following vulnerability:

notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The problem has been patched in the release v1.0.0-rc.3. Some workarounds are available. Users can review their own trust policy file and check if the identity string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`.

CVE-2023-25656 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **notaryproject** - **notation-go** version **< 1.0.0-rc.3**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Release v1.0.0-rc.3 · notaryproject/notation-go · GitHub	github.com text/html	MISC github.com/notaryproject/notation-go/releases/tag/v1.0.0-rc.3
Excessive memory allocation on verification · Advisory · notaryproject/notation-go · GitHub	github.com text/html	MISC github.com/notaryproject/notation-go/security/advisories/GHSA-87x9-7grx-m28v

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that 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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Notation-go Project	Notation-go	0.7.0	alpha1	All	All
Application	Notation-go Project	Notation-go	0.8.0	alpha1	All	All
Application	Notation-go Project	Notation-go	0.9.0	alpha1	All	All

cpe:2.3:a:notation-go_project:notation-go:0.7.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:notation-go_project:notation-go:0.8.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:notation-go_project:notation-go:0.9.0:alpha1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25656 : notation-go is a collection of libraries for supporting Notation sign, verify, push, pull of oci a… twitter.com/i/web/status/1…	2023-02-20 16:03:33
/r/netcve	CVE-2023-25656	2023-02-20 17:38:09

← Previous ID

Next ID→