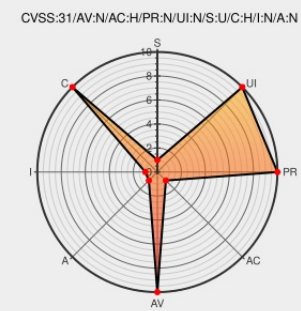
CVE-2023-32691

Published on: Not Yet Published

Last Modified on: 06/05/2023 05:37:00 PM UTC

CVE-2023-32691 - advisory for GHSA-qjrq-hm79-49ww

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



Certain versions of Go Simple Tunnel from Go Simple Tunnel Project contain the following vulnerability:

gost (GO Simple Tunnel) is a simple tunnel written in golang. Sensitive secrets such as passwords, token and API keys should be compared only using a constant-time comparison function. Untrusted input, sourced from a HTTP header, is compared directly with a secret. Since this comparison is not secure, an attacker can mount a side-channel timing attack to guess the password. As a workaround, this can be easily fixed using a constant time comparing function such as `crypto/subtle`'s `ConstantTimeCompare`.

CVE-2023-32691 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **ginuerzh** - **gost** version **= <= 2.11.5**

CVSS3 Score: 5.9 - MEDIUM

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

CVE References

Description	Tags	Link
gost/auth.go at 1c62376e0880e4094bd3731e06bd4f7842638f6a · ginuerzh/gost · GitHub	github.com text/html	MISC github.com/ginuerzh/gost/blob/1c62376e0880e4094bd3731e06bd4f784263
Timing Attack in ginuerzh/gost · Advisory · ginuerzh/gost · GitHub	github.com text/html	MISC github.com/ginuerzh/gost/security/advisories/GHSA-qjrq-hm79-49v

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

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	Go Simple Tunnel Project	Go Simple Tunnel	All	All	All	All

cpe:2.3:a:go_simple_tunnel_project:go_simple_tunnel:*:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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