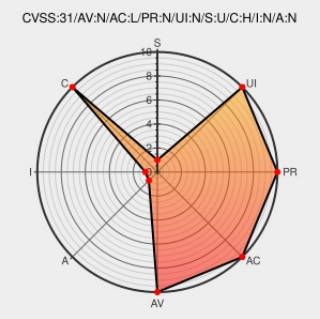
CVE-2015-10004

Published on: Not Yet Published

Last Modified on: 02/28/2023 06:07:17 PM UTC

CVE-2015-10004

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



Certain versions of Json Web Token from Json Web Token Project contain the following vulnerability:

Token validation methods are susceptible to a timing side-channel during HMAC comparison. With a large enough number of requests over a low latency connection, an attacker may use this to determine the expected HMAC.

CVE-2015-10004 has been assigned by security@golang.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **github.com/robbert229/jwt** - **github.com/robbert229/jwt** version **< 0.0.0-20170426191122-ca1404ee6e83**

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	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Merge pull request #13 from polezaivsani/fix_timming_sidechannel · robbert229/jwt@ca1404e · GitHub	github.com text/html	MISC github.com/robbert229/jwt/commit/ca1404ee6e83fcbafb66b09ed0d543850a15b654
Secure problem · Issue #12 · robbert229/jwt · GitHub	github.com text/html	MISC github.com/robbert229/jwt/issues/12
GO-2020-0023 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2020-0023

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	Json Web Token Project	Json Web Token	-	All	All	All

cpe:2.3:a:json_web_token_project:json_web_token:-:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→