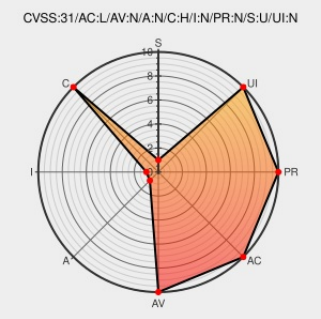
CVE-2020-26160

Published on: 09/30/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-26160

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



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

jwt-go before 4.0.0-preview1 allows attackers to bypass intended access restrictions in situations with []string{} for m["aud"] (which is allowed by the specification). Because the type assertion fails, "" is the value of aud. This is a security problem if the JWT token is presented to a service that lacks its own audience check.

CVE-2020-26160 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Access Restriction Bypass in github.com/dgrijalva/jwt-go | Snyk	Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-GOLANG-GITHUBCOMDGRIJALVAJWTGO-596515

Fix sec vuln with list of claims by Waterdrips · Pull Request #426 · dgrijalva/jwt-go · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/dgrijalva/jwt-go/pull/426

Related QID Numbers

501854 Alpine Linux Security Update for gitea

981838 Go (go) Security Update for github.com/dgrijalva/jwt-go (GHSA-w73w-5m7g-f7qc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jwt-go Project	Jwt-go	All	All	All	All

cpe:2.3:a:jwt-go_project:jwt-go:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@k1LoW	はてなブログに投稿しました #はてなブログ メンテナンスが終了しているgithub.com/dgrijalva/jwt-…の脆弱性CVE-2020-26160に対応する - Copy/Cut/Paste/Hatena k1low.hatenablog.com/entry/2021/09/…	2021-09-05 08:31:28
@sitikantha2018	@andygrunwald The dependency "github.com/dgrijalva/jwt-…" has a vulnerability, CVE-2020-26160. It would be good to upd… twitter.com/i/web/status/1…	2021-09-28 19:01:58

← Previous ID

Next ID→