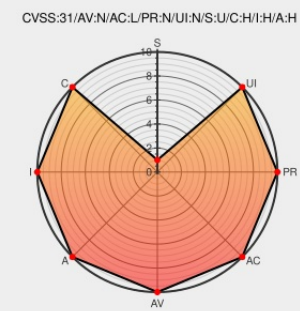
CVE-2017-20146

Published on: Not Yet Published

Last Modified on: 06/12/2023 08:06:26 PM UTC

CVE-2017-20146

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



Certain versions of Handlers from Gorillatoolkit contain the following vulnerability:

Usage of the CORS handler may apply improper CORS headers, allowing the requester to explicitly control the value of the Access-Control-Allow-Origin header, which bypasses the expected behavior of the Same Origin Policy.

CVE-2017-20146 has been assigned by security@golang.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **github.com/gorilla/handlers** - **github.com/gorilla/handlers** version **< 1.3.0**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Don't return the origin header when configured to * by ejcx · Pull Request #116 · gorilla/handlers · GitHub	github.com text/html	MISC github.com/gorilla/handlers/pull/116
[bugfix] Don't return the origin header when configured to * (#116) · gorilla/handlers@9066371 · GitHub	github.com text/html	MISC github.com/gorilla/handlers/commit/90663712d74cb411cbef281bc1e08c19d1a76145
GO-2020-0020 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2020-0020

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	Gorillatoolkit	Handlers	All	All	All	All

cpe:2.3:a:gorillatoolkit:handlers:*:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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