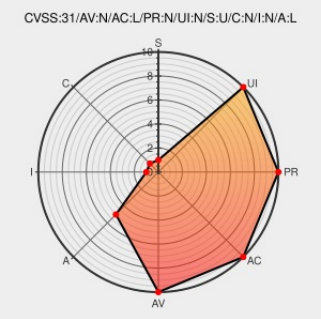
CVE-2021-21328

Published on: 02/25/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:58 PM UTC

CVE-2021-21328 - advisory for GHSA-gcj9-jj38-hwmc

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



Certain versions of Vapor from Vapor Project contain the following vulnerability:

Vapor is a web framework for Swift. In Vapor before version 4.40.1, there is a DoS attack against anyone who Bootstraps a metrics backend for their Vapor app. The following is the attack vector: 1. send unlimited requests against a vapor instance with different paths. this will create unlimited counters and timers, which will eventually drain the system. 2. downstream services might suffer from this attack as well by being spammed with error paths. This has been patched in 4.40.1. The `DefaultResponder` will rewrite any undefined route paths for to `vapor_route_undefined` to avoid unlimited counters.

CVE-2021-21328 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **vapor** - **vapor** version **<= 4.40.0**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Vapor (Web Framework for Swift)	Product vapor.codes text/html	MISC vapor.codes/
Merge pull request from GHSA-gcj9-jj38-hwmc · vapor/vapor@e3aa712 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/vapor/vapor/commit/e3aa712508db2854ac0ab905696c65fd88fa7e23
Release Rewrite metrics path and method to undefined for unknown routes · vapor/vapor · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/vapor/vapor/releases/tag/4.40.1
Vapor's Metrics integration could cause a system drain · Advisory · vapor/vapor · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/vapor/vapor/security/advisories/GHSA-gcj9-jj38-hwmc

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vapor Project	Vapor	All	All	All	All
Application	Vapor Project	Vapor	All	All	All	All

cpe:2.3:a:vapor_project:vapor:*:*:*:*:*:swift:*:*:

cpe:2.3:a:vapor_project:vapor:*:*:*:*:*:swift:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→