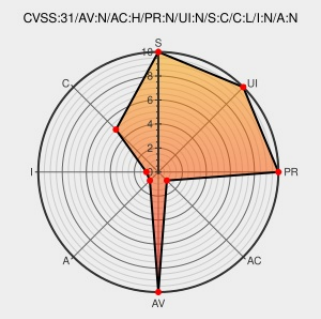
CVE-2021-32822

Published on: 08/16/2021 12:00:00 AM UTC

Last Modified on: 07/02/2022 06:23:00 PM UTC

CVE-2021-32822 - advisory for GHSL-2021-020

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



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

The npm hbs package is an Express view engine wrapper for Handlebars. Depending on usage, users of hbs may be vulnerable to a file disclosure vulnerability. There is currently no patch for this vulnerability. hbs mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration options a file disclosure vulnerability may be triggered in downstream applications. For an example PoC see the referenced GHSL-2021-020.

CVE-2021-32822 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **pillarjs** - **hbs** version **all**

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	LOW	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
GHSL-2021-020: File disclosure in hbs - CVE-2021-32822 | GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2021-020-pillarjs-hbs/

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 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.

Related QID Numbers

981257 Nodejs (npm) Security Update for hbs (GHSA-7f5c-rpf4-86p8)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hbs Project	Hbs	-	All	All	All

cpe:2.3:a:hbs_project:hbs:-:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2021-020: File disclosure in hbs - CVE-2021-32822 github.co/2SzAG8S	2021-05-27 19:50:31
@CVEreport	CVE-2021-32822 : The npm hbs package is an Express view engine wrapper for Handlebars. Depending on usage, users of… twitter.com/i/web/status/1…	2021-08-16 18:50:03

← Previous ID

Next ID→