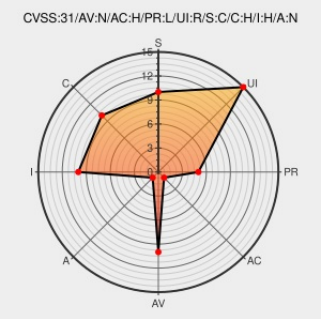
CVE-2021-32818

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 08/12/2021 06:06:00 PM UTC

CVE-2021-32818 - advisory for GHSL-2021-025

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



Certain versions of Haml-coffee from Haml-coffee Project contain the following vulnerability:

haml-coffee is a JavaScript templating solution. haml-coffee mixes pure template data with engine configuration options through the Express render API. More specifically, haml-coffee supports overriding a series of HTML helper functions through its configuration options. A vulnerable application that passes user controlled request objects to the haml-coffee template engine may introduce RCE vulnerabilities. Additionally control over the escapeHtml parameter through template configuration pollution ensures that haml-coffee would not sanitize template inputs that may result in reflected Cross Site Scripting attacks against downstream applications. There is currently no fix for these issues as of the publication of this CVE. The latest version of haml-coffee is currently 1.14.1. For complete details refer to the referenced GHSL-2021-025.

CVE-2021-32818 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **netzpirat** - **haml-coffee** version **<= 1.14.1**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
GHSL-2021-025: Remote code execution and Reflected cross site scripting in haml-coffee - CVE-2021-32818 | GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2021-025-haml-coffee/
haml-coffee - npm	www.npmjs.com text/html	MISC www.npmjs.com/package/haml-coffee

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

982587 Nodejs (npm) Security Update for haml-coffee (GHSA-m7mf-vm62-7x3q)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haml-coffee Project	Haml-coffee	All	All	All	All
Application	Haml-coffee Project	Haml-coffee	All	All	All	All

cpe:2.3:a:haml-coffee_project:haml-coffee:*:*:*:*:*:*:*:*:

cpe:2.3:a:haml-coffee_project:haml-coffee:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2021-025: Remote code execution and Reflected cross site scripting in haml-coffee - CVE-2021-32818 github.co/3eLK4iw	2021-05-14 16:10:09
@CVEreport	CVE-2021-32818 : haml-coffee is a JavaScript templating solution. haml-coffee mixes pure template data with engine… twitter.com/i/web/status/1…	2021-05-14 18:30:08
/r/netcve	CVE-2021-32818	2021-05-14 18:41:30

← Previous ID

Next ID→

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