



CVE-2021-32696

Published on: 06/18/2021 12:00:00 AM UTC

Last Modified on: 06/24/2021 07:20:00 PM UTC

CVE-2021-32696 - advisory for GHSA-qxg5-2qff-p49r

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N



Certain versions of [Striptags](#) from [Striptags Project](#) contain the following vulnerability:

The npm package "striptags" is an implementation of PHP's strip_tags in Typescript. In striptags before version 3.2.0, a type-confusion vulnerability can cause `striptags` to concatenate unsanitized strings when an array-like object is passed in as the `html` parameter. This can be abused by an attacker who can control the shape of their input, e.g. if query parameters are passed directly into the function. This can lead to a XSS.

CVE-2021-32696 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: ericnorris - **striptags** version < 3.2.0

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	LOW	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Description	Tags	Link
striptags - npm	www.npmjs.com text/html	 MISC www.npmjs.com/package/striptags
Release v3.2.0 · ericnorris/striptags · GitHub	github.com text/html	 MISC github.com/ericnorris/striptags/releases/tag/v3.2.0
Merge pull request from GHSA-qxg5-2qff-p49r · ericnorris/striptags@f252a6b · GitHub	github.com text/html	 MISC github.com/ericnorris/striptags/commit/f252a6b0819499cd65403707ebaf5cc925f2faca
Passing in a non-string 'html' argument can lead to unsanitized output · Advisory · ericnorris/striptags · GitHub	github.com text/html	 CONFIRM github.com/ericnorris/striptags/security/advisories/GHSA-qxg5-2qff-p49r

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

[982052](#) Nodejs (npm) Security Update for striptags (GHSA-qxg5-2qff-p49r)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Striptags Project	Striptags	All	All	All	All
cpe:2.3:a:striptags_project:striptags:*:*:*:*:node.js:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-32696 : The npm package "striptags" is an implementation of PHP's strip_tags in Typescript. In striptags b... twitter.com/i/web/status/1...	2021-06-18 19:40:18
 /r/netcve	CVE-2021-32696	2021-06-18 20:41:23

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

