



CVE-2021-23472

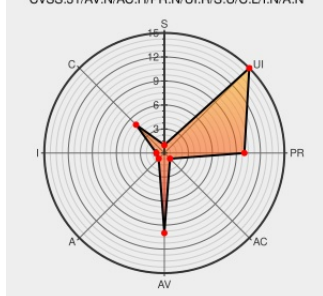
Published on: 11/03/2021 12:00:00 AM UTC

Last Modified on: 01/23/2023 05:14:00 PM UTC

CVE-2021-23472

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

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



Certain versions of [Bootstrap Table](#) from [Bootstrap-table](#) contain the following vulnerability:

This affects versions before 1.19.1 of package bootstrap-table. A type confusion vulnerability can lead to a bypass of input sanitization when the input provided to the escapeHTML function is an array (instead of a string) even if the escape attribute is set.

CVE-2021-23472 has been assigned by report@snyk.io to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Cross-site Scripting (XSS) in bootstrap-table Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-BOOTSTRAPTABLE-1657597
Cross-site Scripting (XSS) in org.webjars.bowergithub.wenzhixin:bootstrap-table Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBWENZHIXIN-1910687

bootstrap-table/index.js at develop · wenzhixin/bootstrap-table · GitHub	github.com text/html	 MISC github.com/wenzhixin/bootstrap-table/blob/develop/src/utils/index.js%23L218
Cross-site Scripting (XSS) in org.webjars.npm:bootstrap-table Snyc	snyk.io text/html	 MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1910688
Cross-site Scripting (XSS) in org.webjars.bower:bootstrap-table Snyc	snyk.io text/html	 MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1910689
Cross-site Scripting (XSS) Snyc	security.snyk.io text/html	 MISC security.snyk.io/vuln/SNYK-JS-BOOTSTRAPTABLE-1657597
Cross-site Scripting (XSS) in org.webjars:bootstrap-table Snyc	snyk.io text/html	 MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1910690

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

[980028](#) Nodejs (npm) Security Update for bootstrap-table (GHSA-mw6q-98mp-g8g8)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bootstrap-table	Bootstrap Table	All	All	All	All
Application	Bootstrap Table Project	Bootstrap Table	All	All	All	All
Application	Bootstrap Table Project	Bootstrap Table	-	All	All	All
cpe:2.3:a:bootstrap-table:bootstrap_table:*****:						
cpe:2.3:a:bootstrap_table_project:bootstrap_table:*****:						
cpe:2.3:a:bootstrap_table_project:bootstrap_table:-*****:						

Discovery Credit

Alessio Della Libera of Snyc Research Team

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23472 : This affects all versions of package bootstrap-table. A type confusion vulnerability can lead to... twitter.com/i/web/status/1...	2021-11-03 17:32:03

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)