



CVE-2021-23682

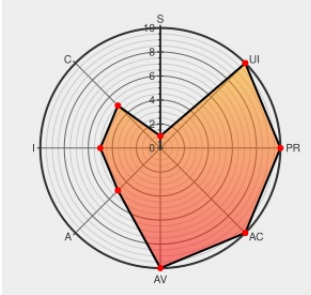
Published on: Not Yet Published

Last Modified on: 02/28/2022 05:50:06 PM UTC

CVE-2021-23682

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

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



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

This affects the package litespeed.js before 0.3.12; the package appwrite/server-ce from 0.12.0 and before 0.12.2, before 0.11.1. When parsing the query string in the getJsonFromUrl function, the key that is set in the result object is not properly sanitized leading to a Prototype Pollution vulnerability.

CVE-2021-23682 has been assigned by report@snyk.io to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Release Version 0.11.1 · appwrite/appwrite · GitHub	Release Notes Third Party Advisory github.com	MISC github.com/appwrite/appwrite/releases/tag/0.11.1

Release Version 0.12.2 · appwrite/appwrite · GitHub	text/html Release Notes Third Party Advisory github.com text/html	 MISC github.com/appwrite/appwrite/releases/tag/0.12.2
Prototype Pollution in litespeed.js CVE-2021-23682 Snyk	Exploit Third Party Advisory snyk.io text/html	 MISC snyk.io/vuln/SNYK-JS-LITESPEEDJS-2359250
fix: prototype vulnerability in router by TorstenDittmann · Pull Request #18 · litespeed-js/litespeed.js · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/litespeed-js/litespeed.js/pull/18
fix: security patches for 0.12.2 by TorstenDittmann · Pull Request #2778 · appwrite/appwrite · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/appwrite/appwrite/pull/2778
Prototype Pollution in appwrite/server-ce CVE-2021-23682 Snyk	Exploit Third Party Advisory snyk.io text/html	 MISC snyk.io/vuln/SNYK-PHP-APPWRITESERVERCE-2401820

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Appwrite	Appwrite	All	All	All	All
Application	Litespeed.js Project	Litespeed.js	All	All	All	All

cpe:2.3:a:appwrite:appwrite:*:*:*:*:*:

cpe:2.3:a:litespeed.js_project:litespeed.js:*:*:*:*:node.js:*:

Discovery Credit

Alessio Della Libera of Snyk Research Team

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23682 : This affects the package litespeed.js before 0.3.12; the package appwrite/server-ce from 0.12.0 an... twitter.com/i/web/status/1...	2022-03-01 00:45:21
 /r/netcve	CVE-2021-23682	2022-03-01 01:38:46

© [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](#).

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