HIGH

Search by package name or CVE

Prototype Pollution

Affecting appwrite/server-ce package, versions >=0.12.0, <0.12.2 <0.11.1

INTRODUCED: 24 JAN 2022   CVE-2021-23682 ⑦   CWE-1321 ⑦   `FIRST ADDED BY SNYK`

Share ⌄

How to fix?

Upgrade `appwrite/server-ce` to version 0.12.2, 0.11.1 or higher.

Overview

appwrite/server-ce is an End to end backend server for frontend and mobile apps.

Affected versions of this package are vulnerable to Prototype Pollution. 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.

PoC

1. add the following query string `?__proto__[polluted]=yes`

2. open the browser developer console. The property `polluted` has value `yes`

References

- appwrite Github PR
- appwrite Github Release 0.11.1
- appwrite Github Release 0.12.2
- litespeed.js Github PR

Snyk CVSS

Exploit Maturity	Proof of concept ⑦
Attack Complexity	Low ⑦

See more

> NVD   9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-PHP-APPWRITESERVERCE-2401820
Published	16 Feb 2022
Disclosed	24 Jan 2022
Credit	Alessio Della Libera of Snyk Research Team

Report a new vulnerability   Found a mistake?

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community