huntr

Stored xss in "users name","functions name","storage buckets name" and in "database collections name" in appwrite/appwrite

1

✓ Valid Reported on Jun 27th 2022

Description

Appwrite application allows malicious javascript payload to inject in users name,functions name,storage buckets name and in database collections name which leads to Stored XSS.

Proof of Concept

1.Login to the application
2.Go to the "users name","functions name","storage buckets name" and in "database collections name" and add the javascript payload.

Payload:

```
<img src=1 onerror=alert(document.location)>
```

3.Then view the created user ,function, storage bucket, database collection now XSS will trigger.

PoC video:

https://drive.google.com/file/d/1JoMQy1KTodVtIVOzH3vKcC3AwZz0PrFb/view?usp=sharing

Impact

This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.

CVE

CVE-2022-2925
(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Critical (9)

Registry
Packagist

Affected Version
0.14.2

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

This report was seen 720 times.

We are processing your report and will contact the **appwrite** team within 24 hours. 5 months ago

SAMPRIT DAS modified the report 5 months ago

We have contacted a member of the **appwrite** team and are waiting to hear back 5 months ago

We have sent a follow up to the **appwrite** team. We will try again in 7 days. 5 months ago

We have sent a second follow up to the **appwrite** team. We will try again in 10 days. 5 months ago

We have sent a third and final follow up to the **appwrite** team. This report is now considered stale. 4 months ago

❤ Jake Barnby gave praise 3 months ago

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Jake Barnby validated this vulnerability 3 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

SAMPRIT DAS 3 months ago Researcher

Hello @abnegate can you please tell me when you will deploy the fix?

Jake Barnby 3 months ago Maintainer

We're planning to release in the next few days, you can track any updates on our releases page

We have sent a fix follow up to the **appwrite** team. We will try again in 7 days. 3 months ago

SAMPRIT DAS 3 months ago Researcher

Okay

SAMPRIT DAS 3 months ago Researcher

@admin As this report is marked as valid can I get the bounty for this report?

Jamie Slome 3 months ago Admin

We are not currently offering bounties for non-sponsored projects 👍

We have sent a second fix follow up to the **appwrite** team. We will try again in 10 days.
3 months ago

A **appwrite/appwrite** maintainer marked this as fixed in **1.0.0-RC1** with com
3 months ago

Chat with us

The fix bounty has been dropped ✗

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us