

## Stored XSS in Task field in kromitgmbh/titra

0



Valid

Reported on Jun 4th 2022

### Description

The application **Titra** is vulnerable to Stored XSS in Task field.

### Steps To Reproduce

Click on add Track button

In the Task field enter the payload `"><img src=# onerror=alert(document.domain)>`

click save

Now Click on Details

XSS will be triggered

### Image PoC

<https://drive.google.com/file/d/1twcYvvdV-hCE4hI0HwtnE9ZvqpYC77gS/view?usp=sharing>

<https://drive.google.com/file/d/1CNtiY-VeLjPtYQOx3clUKSxgSAMM2mQM/view?usp=sharing>

### Impact

This allows the attacker to execute malicious scripts in all the project members browser and it can lead to session hijacking, sensitive data exposure, and worse.

CVE

CVE-2022-2029

(Published)

Vulnerability Type

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

Severity

High (8.2)

Registry

Other

Chat with us

## Affected Version

<=0.76.0

## Visibility

Public

## Status

Fixed

## Found by



saharshtapi

@saharshtapi

master ▼

This report was seen 452 times.

We are processing your report and will contact the **kromitgmbh/titra** team within 24 hours.

6 months ago

saharshtapi 6 months ago

Researcher

@admin please change the vulnerability type from DOM XSS to Stored XSS

saharshtapi modified the report 6 months ago

We have contacted a member of the **kromitgmbh/titra** team and are waiting to hear back

6 months ago

Jamie Slome 6 months ago

Admin

@saharshtapi - you should be able to change the vulnerability type to Stored XSS using the [Edit](#) button at the top right-hand side of the page.

If you are unable to, this is because you already have a Stored XSS report pending against this repository, and so should add the other occurrences of the same vulnerability type to that report using the permalinks.

A **kromitgmbh/titra** maintainer validated this vulnerability 6 months ago

Chat with us

saharshtapi has been awarded the disclosure bounty

saharshtapi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A kromitgmbh/titra maintainer marked this as fixed in 0.77.0 with commit e606b6  
6 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

A kromitgmbh/titra maintainer 6 months ago

Maintainer

thanks for reporting this!

saharshtapi 6 months ago

Researcher

@admin Can you assign CVE?

Jamie Slome 6 months ago

Admin

Sorted 👍

Sign in to join this conversation

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[about](#)

[team](#)

[Chat with us](#)