huntr

Stored XSS in Task field in kromitgmbh/titra

0



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 ">
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

Affected Version Visibility Status Found by saharshtapi master 🗸 We are processing your report and will contact the kromitgmbh/titra team within 24 hours. 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

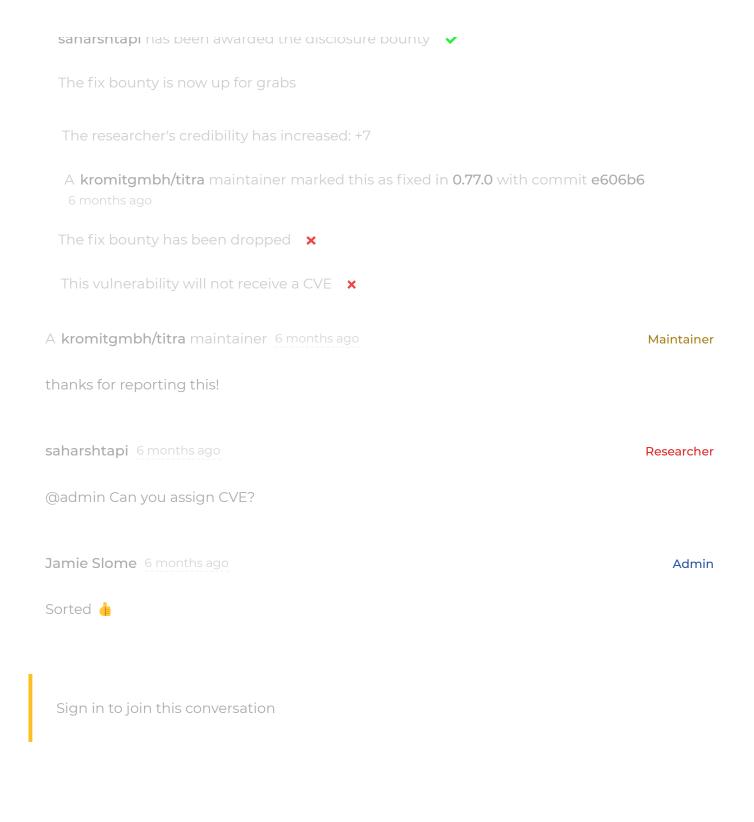
Jamie Slome 6 months ago

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



2022 © 418sec

huntr home

part of 418sec

hacktivity about leaderboard team

FAO

contact us

terms

privacy policy