Stored XSS in Project Name in kromitgmbh/titra

0

Valid Reported on Jun 4th 2022

Description

The application `Titra` is vulnerable to Stored XSS in Project name field.

Steps To Reproduce

Click on Edit button
Under the Project Name enter the paylaod `"><img src=# onerror=alert(document.domain)>`
Click on save.
Now navigate to details the XSS will be triggered.

Image PoC

https://drive.google.com/file/d/1P44bIq0VgqMMUdb7VEKhF1Q_7PdY2k4Z/view?usp=sharing
https://drive.google.com/file/d/1sEJnrY8wxPY9gw1yPL1M4NH7Xe0qkgMT/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-2022-2028
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Generic

Severity
High (8.2)

Registry
Other

Affected Version
<=0.76.0

Visibility
Public

Status
Fixed

Found by

saharshtapi
@saharshtapi
master

This report was seen 432 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 Generic XSS to Stored XSS

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

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 gave praise 6 months ago

thanks for reporting this!

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

saharshtapi 6 months ago — Researcher

@admin Can you assign CVE?

Jamie Slome 6 months ago — Admin

Sorted 👍

> Sign in to join this conversation