Stored XSS in Name in kromitgmbh/titra

0

Valid Reported on Jun 3rd 2022

Description

The application `Titra` is vulnerable to Stored XSS in user's name field.

Proof of Concept

Go to profile and under the name put the payload `"><img src=# onerror=alert(document.domain)>` Video POC: https://drive.google.com/file/d/1MHPloy-i2hsxaLuuVn46oUZVpFm6Nywf/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-2022-2026
(Published)

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

Severity
High (8.2)

Registry
Npm

Affected Version
<=0.76.0

Visibility
Public

Status
Fixed

Found by

saharshtapi

@saharshtapi

master

This report was seen 517 times.

We are processing your report and will contact the **kromitgmbh/titra** team within 24 hours. 6 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 6 months ago

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

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 maintai

saharshtapi 6 months ago Researcher

@admin Can you assign CVE?

Jamie Slome 6 months ago Admin

Sorted 👍

> Sign in to join this conversation