# Mass Assignment in Self Controller Leads To Vertical Privillege Escalation in budibase/budibase

0

Valid Reported on Sep 10th 2022

## Description

Hello there, y'all! How are you doing? Hope you are doing great!

I was testing Budibase and noticed that the api endpoint `/api/global/self`, which is used for different purposes (updating an user's name or their password), always receives an entire object containing most of the attributes of a user, including this user's roles. So by reading the code, I noticed that this "self update" process had a mass assignment, in which the only thing we cannot change is our own ID, but we can change our access level and become the admin of any tenant we belong to.

In other words, whenever an admin invites people to be app users, there's a risk that one of these app users change their role to admin and then make the original admin a simple app user, being now capable of doing anything they would want to, including destroy all of a tenant apps or change their content to something else.

## Steps to Reproduce

1 => Create a user that will be the admin of a tenant, and then invite a second email to be an app user;
2 => Now, as the invited user (possible attacker), login and click on `Update user information`. This modal is supposed to change only a user's name, but if you use a proxy tool such as Burpsuite or OWASP Zap, you can intercept the request that's being sent;
3 => With the request being intercepted, change the attributes `builder`, `admin` and `accountPortalAccess` that are in the JSON object, to something like this:

```
{
...
    "builder": {
        "global":true
```

Chat with us

```
    },
    "admin": {
        "global":true

    },
...
    "accountPortalAccess":true,
...
}
```

4 => Boom! Now, if you log out and in, you will see the same dashboard that only editors and admins can see, `and you can even go to the users page and change the role of the original admin to a lower one` ;

## Impact

Whenever an admin invites people to be in their tenant, there's a risk that one of these app users change their own role to admin and then make the original admin a simple app user, being now capable of doing anything they would want to, including destroy all of a tenant apps or change their content to something else.

## Occurrences

JS self.js L138

It's clear here that it picks up `the entire request body` and use it to update the user!

CVE
CVE-2022-3225
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (8.8)

Registry
Other

Affected Version

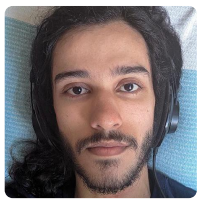
Chat with us

<=1.3.11

Visibility
Public

Status
Fixed

Found by



Breno Vitório
@brenu
legend

This report was seen 820 times.

We are processing your report and will contact the **budibase** team within 24 hours. 3 months ago

**Breno Vitório** modified the report 3 months ago

We have contacted a member of the **budibase** team and are waiting to hear back 2 months ago

We have sent a follow up to the **budibase** team. We will try again in 7 days. 2 months ago

A **budibase/budibase** maintainer gave praise 2 months ago

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

A **budibase/budibase** maintainer validated this vulnerability 2 months ago

**Breno Vitório** has been awarded the disclosure bounty

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **budibase/budibase** maintainer marked this as fixed in **1.3.20** with commit **d35864**
2 months ago

The fix bounty has been dropped

This vulnerability will not receive a CVE

Chat with us

self.js#L138 has been validated ✔

nuno 7 days ago

@admin Was reported in August 8 at https://huntr.dev/bounties/077eda41-517b-4e60-bd0c-b72b8ea48b0c/

Sign in to join this conversation

2022 © 418sec



Chat with us