huntr

Authorization Bypass Through User-Controlled Key in elgg/elgg

0

✓ Valid Reported on Nov 11th 2021

Hello there! Hope you're having an awesome day :D

Actually, it's been a few months since I found this bug, but I had no success in trying to contact you guys, and now I discovered that you're on Huntr. So now I'm sending my report from here :)

Summary

During this week, I was participating at a bug bounty beginners event and they used Elgg to create a social network example. So...I ended up submitting a report, thinking that it might be an on purpose bug, but it was actually a bug on the Elgg itself, because I installed it on my computer and it still happens.

Basically, the bug is an IDOR on the endpoints below:

```
https://website-example.com/action/groups/join
https://website-example.com/action/groups/leave
```

These endpoints request a param called `user_guid` , which represents the user that will be joining or leaving the group. But also, these endpoints don't filter whether the request is being made by the user itself or not, and because of that, any user is able to intercept the HTTP request and change the `user_guid` param to any other user ID, in a way that's possible to create a group and add people to it without needing to invite them, or maybe worse than that, it's possible to pick a group that already exists and remove everyone from it (except the group owner) without having enough permissions.

STEPS TO REPRODUCE

1 => Let's begin from an Elgg example instance (I've tested on 3.3.21, and maybe previous versions are also vulnerable to that);
2 => Besides the admin user, create two other users (with three different users, we will have the group owner, the "attacker" and the "victim");
3 => Logged into UserA, create a group. UserA will be the group owner;
4 => Logged into UserB (attacker), go to the profile page of the UserC (victim);
5 => As the UserB, pick up UserC's ID (there are some buttons inside the profile page that show up the user ID, as for example, the "Add friend" button and the "Send a message" button);
6 => Now that UserB has the victim's ID, go to the page of UserA's group;
7 => At this point, maybe you'll need a tool to intercept your own HTTP requests before testing the bug, I used Burpsuite but you guys may test it with any other tool;
8 => With your intercept tool turned on, and looking to the group page as the UserB, click on the "Join group" button and intercept the HTTP request.
9 => Looking at the request URL, you will see a param called "user_guid", which at this moment has the UserB's ID. Replace it with UserC's (victim) ID and forward the request.
10 => The endpoint will return a message telling that UserB succesfully joined the group, but when you look at the group members list, the Victim is the one who joined the group.
11 => These steps are the same for testing the /action/leave endpoint, but the victim ID must be from an user that's already a group member.

POSSIBLE SOLVING WAYS

Probably you guys already know how to solve an IDOR like that, but I would like to point two possibilites:

1 => Verify if the `user_guid` param is really equal to the id of the user who's requesting these group actions;
2 => Instead of requesting the user ID as a param, the endpoint could also be picking it automatically from the database or from the user session;

References

- More about this CWE

CVE
CVE-2021-3964
(Published)

Vulnerability Type
CWE-639: Authorization Bypass Through User-Controlled Key

Severity
Medium (4.3)

Chat with us

Visibility
Public

Status
Fixed

Found by

Breno Vitório
@brenu
legend

This report was seen 453 times.

We are processing your report and will contact the **elgg** team within 24 hours. a year ago

Breno Vitório modified the report a year ago

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

We have contacted a member of the **elgg** team and are waiting to hear back a year ago

Breno Vitório a year ago — Researcher

I decided to test for this new stable version of Elgg, which is on the branch 4.x, and it's still vulnerable. So I created a fork and fixed it for both branches 4.x and 3.3.

Breno Vitório submitted a **patch** a year ago

Breno Vitório submitted a **patch** a year ago

A **elgg/elgg** maintainer validated this vulnerability a year ago

Breno Vitório has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **elgg/elgg** maintainer a year ago

Some validation needs to be added that the current user is allowed to execute the actions. Simply changing the user_guid to the current user fixes the issue, but also breaks functionality.

A **elgg/elgg** maintainer a year ago

fixed with https://github.com/Elgg/Elgg/pull/13776

Breno Vitório a year ago — Researcher

Oh, I see. Thank you for validating and fixing the issue!

Breno Vitório a year ago — Researcher

As a security update was already released for this issue, may we change its status to fixed?

A **elgg/elgg** maintainer marked this as fixed in **3.3.22** with commit **d9fcad** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago — Admin

CVE published! 🎉

Sign in to join this conversation