

## Non members can add spent time and reset spent time from issues created by themselves- API

[HackerOne report #755188](#) by ashish\_r\_padelkar on 2019-12-10, assigned to [@akelly](#):

### Summary

Hello,

As per this [https://docs.gitlab.com/ee/user/project/time\\_tracking.html](https://docs.gitlab.com/ee/user/project/time_tracking.html)

Adding time entries (time spent or estimates) is limited to project members

However, if the issue is created by non members themselves in a public project, they can add spent time and reset the spent time using APIs

1. <https://docs.gitlab.com/ee/api/issues.html#add-spent-time-for-an-issue>
2. <https://docs.gitlab.com/ee/api/issues.html#reset-spent-time-for-an-issue>

### Steps to reproduce

1. Create a issue as a non member in public project.
2. If you try to use quick actions like /Spend , it wont work
3. Now try below API

```
curl --request POST --header "PRIVATE-TOKEN: <Token>" https://gitlab.com/api/v4/projects/<ProjectID>/issues/<YourIssueID>/time_entries
```

This will add 1h to your own issue

4. You can also RESET the time spent by project members using below API as a non member.

```
curl --request POST --header "PRIVATE-TOKEN: <Token>" https://gitlab.com/api/v4/projects/<ProjectID>/issues/<YourIssueID>/time_entries/:id
```

### What is the current *bug* behavior?

Allows non members to add/remove spent time on issues created by them

### What is the expected *correct* behavior?

These 2 actions shouldn't be allowed using API too for non members

### Output of checks

This bug happens on GitLab.com and might be on omnibus installations too. This is tested on gitlab.com

Regards,

Ashish

### Impact

Non members can add/remove spent time on issues created by themselves using API

📁 Drag your designs here or [click to upload](#)

**Tasks** 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

**Linked items** 1

**Relates to**

[Unauthorized time entry added via API](#)

#34765

🕒 12.7 🗨 2 📅 Jan 23, 2020 🏷

### Activity

[GitLab SecurityBot](#) added [HackerOne](#) [security](#), labels 2 years ago

[GitLab SecurityBot](#) added [priority 3](#) [severity 3](#), scoped labels 2 years ago

[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 2 years ago

[Author](#) [Reporter](#)

[HackerOne comment](#) by ashish\_r\_padelkar:  
  
Also  
  
These 2 works for same reason  
  
Set/Reset time estimates  

1. <https://docs.gitlab.com/ee/api/issues.html#set-a-time-estimate-for-an-issue>
2. <https://docs.gitlab.com/ee/api/issues.html#reset-the-time-estimate-for-an-issue>

  
Regards, Ashish

[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 2 years ago

[Author](#) [Reporter](#)

[HackerOne comment](#) by akelly:  
  
Hello @ashish\_r\_padelkar,  
  
Thanks for reporting this issue. Unfortunately, it is a duplicate of a previous report that we are tracking at [#34765 \(closed\)](#). The original report will be made public 30 days after a patch is released. Because the GitLab issue will be made public after release, we do not typically add reporters as contributors to the original reports on HackerOne.  
  
Best regards, Andrew Security Team | GitLab

[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 2 years ago


[Author](#) [Reporter](#)

[HackerOne comment](#) by ashish\_r\_padelkar:  
  
Hello @jakelly,  
  
Original of this has been marked as resolved but this isnt resolved yet. Are you sure they are same?  
  
I tested this on GitLab Enterprise Edition 12.7.0-ee now `time_estimate` endpoint and it still works. I did not test other endpoints but they should work too i guess.  
  
Please evaluate this report again.  
  
Regards, Ashish

[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 2 years ago

[Author](#) [Reporter](#)

[HackerOne comment](#) by ashish\_r\_padelkar:  
  
Hello @jakelly,  
  
Can you please look into this again? This is not fixed!  
  
Also a suggestion ,that you guys should add duplicate reporter in original otherwise case like this happens. Reporter has to wait till original marked as resolved just to know that reports arent same. Also gitlab takes 3-6 months average time to resolve any issues and to wait that long requires lot of patience.  
  
And after knowing that reports aren't same, we dont get reply on closed reports and have to comment repeatedly to get any attention on reports.  
  
Regards, Ashish




GitLab SecurityBot @gitlab-securitybot · 2 years ago

AuthorReporter

HackerOne comment

by ashish\_r\_padelkar:

Gitlab closed the report as duplicate of the report which is resolved(i can check my logs) but my report is still working. I think this was not correctly referenced as the bug still exists



GitLab SecurityBot @gitlab-securitybot · 2 years ago

AuthorReporter


HackerOne comment

by ashish\_r\_padelkar:

Hello @jakelly ,

Can i get your attention on this report please?

Regards, Ashish



GitLab SecurityBot @gitlab-securitybot · 2 years ago

AuthorReporter

HackerOne comment

by akelly:

Hi @ashish\_r\_padelkar,

Thanks for following up on this report. We appreciate the time and effort you have put into this and your other findings.


I believe you may be correct that this is not a duplicate as determined initially. I am reopening this report so that I can investigate and will get back to you by the end of this week.

Have a nice day. Andrew Security Team | GitLab

Andrew Kelly marked this issue as related to #34765 (closed) 2 years ago

Andrew Kelly added group project management / discuss plan scoped labels 2 years ago

Andrew Kelly changed due date to April 28, 2020 2 years ago



Andrew Kelly @ankelly · 2 years ago


Developer

Confirmed on 12.7.0, as a non-member I was able to update the time spent and reset it for issues that I had submitted.

edit: I should note that from my perspective, the security impact here is being able to reset the time spent. The fact that it only works for issues the user themselves has submitted is a notable mitigating factor, overall the opportunity for abuse here seems low.

/cc @qweaver and @johnhope

Edited by Andrew Kelly 2 years ago



John Hope @johnhope · 2 years ago

Developer

Thanks @ankelly!

Please register or sign in to reply

John Hope changed milestone to %13.0 2 years ago


John Hope added bug backend labels 2 years ago

John Hope added workflow planning breakdown scoped label 2 years ago

GitLab Bot added accepting merge requests label 2 years ago

Costel Maxim mentioned in issue #34765 (closed) 2 years ago

Andrew Kelly mentioned in issue gitlab-com/git-security/engineering#926 2 years ago



Heinrich Lee Yu @erowan · 2 years ago

Maintainer

It looks like we're checking the wrong permissions in the API endpoints for time tracking. Something like this should probably fix it:

```
diff --git a/lib/api/time_tracking_endpoints.rb b/lib/api/time_tracking_endpoints.rb
index 93fe0bec27..d031f65408 100644
--- a/lib/api/time_tracking_endpoints.rb
+++ b/lib/api/time_tracking_endpoints.rb
@@ -15,7 +15,7 @@ module API
   end

   def update_issuable_key
     - "update_#{issuable_name}".to_sym
     + "admin_#{issuable_name}".to_sym
   end

   def read_issuable_key
```

The update\_xxx permission is for allowing authors and assignees to update the title and description. admin\_xxx is used for updating other parts of an issuable.

Looking at this file, this vulnerability also applies to the .../time\_estimate and .../reset\_time\_estimate endpoints.

I think it's also a good idea to rename update\_issuable\_key to admin\_issuable\_key 🙏

Edited by Heinrich Lee Yu 2 years ago

Heinrich Lee Yu changed weight to 2 2 years ago

Heinrich Lee Yu added breakdown Sufficient label 2 years ago

John Hope mentioned in issue plan#96 (closed) 2 years ago

John Hope changed milestone to %13.1 2 years ago

Donald Cook mentioned in issue plan#107 (closed) 2 years ago

Eugenia Grieff assigned to @eqrieff 2 years ago


Eugenia Grieff added workflow in dev scoped label and automatically removed workflow planning breakdown label 2 years ago

GitLab Bot removed accepting merge requests label 2 years ago

Eugenia Grieff added workflow in review scoped label and automatically removed workflow in dev label 2 years ago

Eugenia Grieff added workflow verification scoped label and automatically removed workflow in review label 2 years ago

GitLab SecurityBot added security-issue-escalated label 2 years ago




GitLab SecurityBot @gitlab-securitybot · 2 years ago

AuthorReporter

@qweaver @leaz @donaldcook @cmaxim This -53 security issue's milestone has expired.

About this automation: AppSec Escalation Engine

Gabe Weaver changed milestone to %13.2 2 years ago



Costel Maxim @cmaxim · 2 years ago

Developer

Issue fixed in 13.1.2

Costel Maxim closed 2 years ago

GitLab SecurityBot removed security-issue-escalated label 2 years ago



**GitLab SecurityBot** @gitlab-securitybot · 2 years ago

Author

Reporter

This [disclosure](#) [was closed](#) 30 days ago and may become public.

Please ensure the following items are true and add a ☒ reaction:

- Issue description and comments do not contain sensitive data belonging to GitLab.
- Issue does not reveal private information of the reporter (i.e. session IDs, passwords).

If the issue needs to stay confidential, please add the [keep confidential](#) label.

If you removed confidential data from the issue description before making it public, make sure that the description history entry is deleted.



**Costel Maxim** @cmaxim · 2 years ago

Developer

Making issue public.



**Costel Maxim** made the issue visible to everyone 2 years ago



**Costel Maxim** @cmaxim · 2 years ago

Developer

Assigned CVE id for this issue: CVE-2020-13319

Please [register](#) or [sign in](#) to reply