Closed · Issue created 2 years ago by GitLab SecurityBot

Group Maintainers can Create/Delete Deploy tokens using API

HackerOne report #828154 by `ashish_r_padelkar` on 2020-03-24, assigned to @dcouture:

Summary

Hello,

New API release in 12.9 of Deploy tokens,A group maintainer is able to create/delete group deploy tokens which i think is not intended. These create/delete functionality is only available to group owners in group settings in UI.

`https://docs.gitlab.com/ee/api/deploy_tokens.html#create-a-group-deploy-token`

Steps to reproduce

1. As a group maintainer, just run the below API

```
curl --request POST --header "PRIVATE-TOKEN: <Token>" --header "Content-Type: application/json" --data '{"name": "My deploy token", "expires_at": "2098-02-02", "username": "custom-user", "scopes": ["read_repository"]}' "https://gitlab.com/api/v4/groups/<ID>/deploy_tokens/"
```

2. This will create a group level deploy token.

3. You can also delete the tokens created by group admin using below API

```
curl --request DELETE --header "PRIVATE-TOKEN: <Token>" "https://gitlab.com/api/v4/groups/<ID>/deploy_tokens/<ID>"
```

What is the current *bug* behavior?

Group Maintainers are able to create/delete group deploy tokens

What is the expected *correct* behavior?

Group Maintainers shouldnt be allowed to create /delete deploy tokens

Output of checks

This bug happens on GitLab.com and probably on omnibus installations too!

Regards,
Ashish

Impact

Group Maintainers are able to create/delete deploy tokens

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 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Activity

GitLab SecurityBot added priority 3 severity 3 scoped labels 2 years ago

GitLab SecurityBot added HackerOne security labels 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago (Author) (Reporter)
HackerOne comment by `dcouture`:

Hello [@]ashish_r_padelkar,

Thanks for your report. I'm going to reach out to the engineering team to see if it's a UI bug or a permission bug and will keep you updated.

Best regards, Dominic GitLab Security Team

Dominic Couture @dcouture · 2 years ago (Developer)
Slack discussion that followed: https://gitlab.slack.com/archives/CSTPFMVQQ/p1585065181086200

Etienne Baqué @ebaque · 2 years ago (Maintainer)
From this Slack conversation, about this bug:

"Maintainers can destroy group tokens via API, and only group owners can do that via the UI (and they're the only one to be able to access group settings for that matter).

Regarding permission-related issues, I use the permissions tables in the docs as SSOT. For this situation, this table is the relevant one.

Based on this table, it looks like the group token API would be too permissive."

Please register or sign in to reply

Dominic Couture added group release devops::release scoped labels 2 years ago

Dominic Couture @dcouture · 2 years ago (Developer)
Hello @ogolowinski and @csouthard! The group token REST API allows maintainers to create and delete tokens while it should be restricted only to group owners. The UI checks the permissions correctly.

Orit Golowinski @ogolowinski · 2 years ago (Developer)
@csouthard @ebaque I am scheduling this for 13.0. Please let me know if you disagree

Orit Golowinski changed milestone to %13.0 2 years ago

GitLab Bot added Accepting merge requests label 2 years ago

Orit Golowinski mentioned in issue #212773 (closed) 2 years ago

GitLab Bot mentioned in issue #212787 (closed) 2 years ago

Orit Golowinski added Category:Continuous Delivery label 2 years ago

Orit Golowinski mentioned in issue progressive_delivery#1 2 years ago

Orit Golowinski mentioned in issue progressive_delivery#2 2 years ago

Orit Golowinski mentioned in issue gitlab-org/ci-cd/progressive_delivery#1 (closed) 2 years ago

Orit Golowinski mentioned in issue #215759 (closed) 2 years ago

Etienne Baqué changed weight to **1** 2 years ago

Orit Golowinski changed milestone to %13.1 2 years ago

Orit Golowinski added ci-cd active Release P2 scoped labels 2 years ago

Etienne Baqué @ebaque · 2 years ago (Maintainer)
Weight estimate: 1

- MR to restrict API: maintainers should not be able to create/destroy group tokens via API

Chase Southard added workflow ready for development scoped label 2 years ago

Chase Southard mentioned in issue gitlab-org/ci-cd/progressive_delivery#4 (closed) 2 years ago

Etienne Baqué @ebaque · 2 years ago — Maintainer

@csouthard I can see that this issue is workflow ready for development and unassigned. If you're ok with it, I can take over it since I know what it is about + I know the whole security bug process. Please let me know.

Chase Southard @csouthard · 2 years ago — Developer

That sounds good to me @ebaque

Please register or sign in to reply

Etienne Baqué assigned to @ebaque 2 years ago

Etienne Baqué added workflow in dev scoped label and automatically removed workflow ready for development label 2 years ago

Etienne Baqué mentioned in merge request !34674 2 years ago

GitLab Bot removed Accepting merge requests label 2 years ago

Etienne Baqué added workflow in review scoped label and automatically removed workflow in dev label 2 years ago

Etienne Baqué @ebaque · 2 years ago — Maintainer

Async Issue Update

Status

- **Complete:** `100%`
- **Confidence:** `95%`

Notes

Done and reviewed. Assigned to the release bot for automatic release (this upcoming Friday)

Merge Requests

Security MR

Orit Golowinski @ogolowinski · 2 years ago — Developer

@ebaque is this part of 13.1 or should it move out to 13.2?

Etienne Baqué @ebaque · 2 years ago — Maintainer

@ogolowinski This is part of 13.1. It's a security fix that target 12.10.x, 13.0.x and 13.1.x https://gitlab.com/gitlab-org/gitlab/-/issues/219305

Please register or sign in to reply

Etienne Baqué 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 — Author, Reporter

@ogolowinski @csouthard @nicolewilliams @dcouture This ~S3 security issue's milestone has expired.

About this automation: AppSec Escalation Engine

Dominic Couture @dcouture · 2 years ago — Developer

The fix is being deployed, the issue will be closed shortly.

Please register or sign in to reply

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

Chase Southard mentioned in issue gitlab-org/ci-cd/progressive_delivery#6 (closed) 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago — Author, Reporter

This HackerOne security issue 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

Please register or sign in to reply