Service desk email address of a project is being leaked through graphql to non-members of the project even If a custom suffix is set for the same.

HackerOne report #1439254 by albatraoz on 2022-01-02, assigned to @cmaxim:

Report | Attachments | How To Reproduce

Report

Summary

I've <u>reported</u> this vulnerability previously too but closed it as N/A myself as the service desk email address is guessable If we have a project name. But this time I saw some activity on gitlab <u>issues</u> about the visibility & it has been changed to <u>reporter</u> & also If any project owner decides to add suffix to their service desk email address to defend the spam, that too would be exposed through graphql.

Steps to reproduce

- 1. Visit https://gitlab.com/-/graphql-explorer
- 2. Put the following graphql query and hit play

```
query{
  project(fullPath:"gitlab-org/gitlab") {
   id
    serviceDeskAddress
  }
}
```

You will see the internal service desk email of the project in the response.

```
{
  "data": {
    "project": {
        "id": "gid://gitlab/Project/278964",
        "serviceDeskAddress": "contact-project+gitlab-org-gitlab-278964-issue-[@]incoming.gitlab.com"
     }
  }
}
```

What is the current bug behavior?

Service desk email address is visible to non members of a project.

What is the expected correct behavior?

Service desk email address should be visible only to members of a project with minium reporter level access.

Relevant logs and/or screenshots

Issue references

#345692 (closed) !74179 (merged)

Impact reference

#329446 (comment 563640175)

Impact

Even though the service desk email address is guessable If we have the project name, If the owner decides to add a secret suffix only visible & shared with project members, the email address would be leaked to non members through graphql. This can lead to issue spam or vandalism of a project.

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

• GraphiQL.png

How To Reproduce

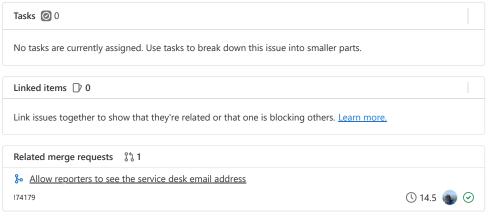
Please add <u>reproducibility information</u> to this section:

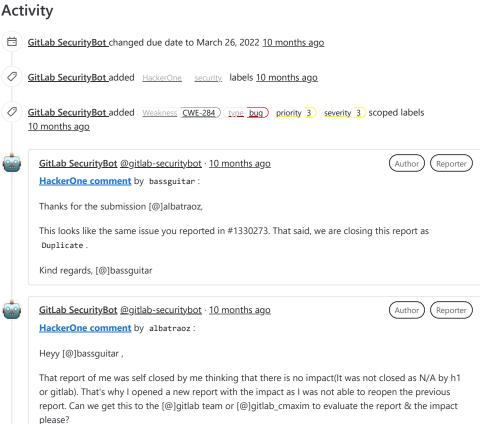
Thanks & Regards, [@]albatraoz

GitLab SecurityBot @gitlab-securitybot · 10 months ago

- 1.
- 2.
- 3.

1 Drag your designs here or click to upload.





(Author) (Reporter)



HackerOne comment by albatraoz:

Any update?



GitLab SecurityBot @gitlab-securitybot · 10 months ago



Reporter

<u>HackerOne comment</u> by albatraoz:

The triager thought that the original report of me of which this report is marked as duplicate as closed as N/A by gitlab or h1. But the original report was my report & I closed it by myself because I was not able to prove impact. But now I'm able to prove impact for the same report but I was not able to reopen the previous report so I wrote this new report with the impact. The triager marked this report as duplicate of my own report which is funny. I'd suggest to go through this report once again through an h1 triager or someone from the gitlab team.



<u>GitLab SecurityBot</u> @gitlab-securitybot · 10 months ago



(Reporter

<u>HackerOne comment</u> by bassguitar:

Hi [@]albatraoz,

Thank you for your report. We appreciate the time and effort spent in putting this report together, however we want to make you aware that Mediation should only be used in cases when all normal discussions with the HackerOne team have been attempted and there has been no satisfactory resolution. More information about Mediation is available here:

Please respect the guidelines above and only request mediation if it's deemed absolutely necessary. We also recommend taking a moment to review the HackerOne Code of Conduct: https://www.hackerone.com/policies/code-of-conduct

Kind regards, [@]bassguitar



GitLab SecurityBot @gitlab-securitybot · 10 months ago



Reporter

HackerOne comment by albatraoz:

Hey [@]bassguitar,

I thought once the report gets closed as duplicate the communication doesn't go through properly & that's why opened a mediation request. I will make sure it doesn't happen again. Hope this report gets revaluated asap.

Thanks & Regards, [@]albatraoz



Costel Maxim added group product planning devops plan scoped labels 10 months ago



Costel Maxim @cmaxim · 10 months ago



FYI: @mjwood @johnhope this is similar to #342823 (closed) just that the email address is leaked via GraphQL.



John Hope @johnhope · 10 months ago



I think this should be a relatively straightforward fix so proposing it for %14.8. Thanks @cmaxim.

Edited by John Hope 10 months ago

Please register or sign in to reply



GitLab SecurityBot @gitlab-securitybot · 10 months ago



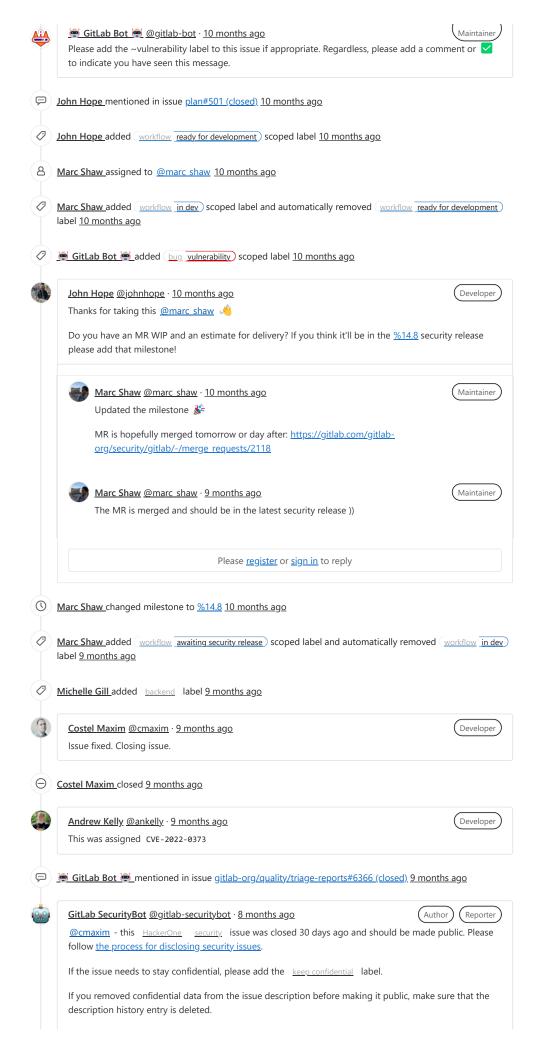
@cdybenko @johnhope @donaldcook @cmaxim This issue is ready for triage as per HackerOne process.

About this automation: AppSec Escalation Engine





GitLab Bot added section dev scoped label 10 months ago



© Costel Maxim made the issue visible to everyone 8 months ago

Please <u>register</u> or <u>sign in</u> to reply