OpenSSH 远程代码执行漏洞(CVE-2024-6387)通告

■ **通告编号**	**NS-2024-0020**	■ 发布日期	**2024-07-01**
■ **漏洞危害**	**攻击者利用此漏洞，可实现远程代码执行。**		
■ **TAG**	OpenSSH、条件竞争、CVE-2024-6387		

一. 漏洞概述

近日，绿盟科技 CERT 监测到 OpenSSH 发布安全公告，修复了 OpenSSH 远程代码执行漏洞(CVE-2024-6387)；由于默认配置下的 OpenSSH Server (sshd)中存在信号处理程序竞争条件问题，如果客户端未在 LoginGraceTime 秒内（默认情况下为 120 秒，旧版 OpenSSH 中为 600 秒）进行身份验证，则 sshd 的 SIGALRM 处理程序将被异步调用，该信号处理程序会调用各种非 async-signal-safe 的函数（例如 syslog()），未经身份验证的攻击者可以利用此漏洞在基于 glibc 的 Linux 系统上以 root 身份执行任意代码。目前漏洞细节与 PoC 已公开，请受影响的用户尽快采取措施进行防护。

OpenSSH 是 SSH （Secure SHell） 协议的免费开源实现。SSH 协议族可以用来进行远程控制， 或在计算机之间传送文件。

参考链接：

https://www.openssh.com/txt/release-9.8

二. 影响范围

受影响版本

- 8.5p1 <= OpenSSH < 9.8p1

注：此漏洞为 2020 年 10 月对 CVE-2006-5051 的重新引入；

不受影响版本

- OpenSSH >= 9.8/9.8p1

注：4.4p1 <= OpenSSH < 8.5p1 不易受到该漏洞攻击，OpenBSD 系统不受该漏洞影响。

三. 漏洞检测

3.1 人工检测

由于更新 OpenSSH 版本可能会有新老版本共存的情况，为保证版本检测的准确性，用户可使用如下命令查看当前使用的 OpenSSH 版本，判断是否在影响范围内：

```
ssh -V
```

```
[root@localhost Desktop]# ssh -V
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
[root@localhost Desktop]#
```

四. 漏洞防护

4.1 官方升级

目前官方发布新版本与安全补丁修复此漏洞，请受影响的用户尽快安装更新进行防护，下载链接：https://www.openssh.com/releasenotes.html

补丁链接：https://github.com/openssh/openssh-portable/commit/81c1099d22b81ebfd20a334ce986c4f753b0db29

Redhat：https://access.redhat.com/security/cve/CVE-2024-6387

Ubuntu：https://lists.ubuntu.com/archives/ubuntu-security-announce/2024-July/008406.html

4.2 临时防护措施

如果 sshd 无法更新或重新编译，可在配置文件中将 LoginGraceTime 设置为 0，此措施会耗尽所有 MaxStartups 连接，从而使 sshd 容易受到拒绝服务攻击，但可以缓解该 RCE 漏洞风险。

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。