安全通告

OpenSSH 远程代码执行漏洞

漏洞预警通报

发布日期：2024-07-04

漏洞描述

2024 年 7 月 4 日公司监测到 openssh 官网发布了 OpenSSH 存在远程代码执行漏洞的更新通告。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，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。该漏洞源于信号处理程序中存在竞争条件，攻击者利用该漏洞可以在无需认证的情况下远程执行任意代码并获得系统控制权。

漏洞编号

CVE-2024-6387

漏洞危害

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。

漏洞等级

严重

影响范围：

OpenSSH < 4.4p1(除非针对 CVE-2006-5051 和 CVE-2008-4109 进行了补丁修复)

8.5p1 <= OpenSSH < 9.8p1

修复方案

目前该漏洞已在官方最新版本中进行了更新修复，请相关用户尽快升级到最新版本。

链接如下：

https://www.openssh.com/releasenotes.html

参考链接

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