防火墙FW、入侵检测IPS、负载均衡LB是否涉及OpenSSH存在远程代码执行漏洞（CVE-2024-6387）

漏洞相关 **刘昆** 21小时前 发表

漏洞相关信息

漏洞编号： CVE-2024-6387
漏洞名称： OpenSSH存在远程代码执行漏洞
产品型号及版本： 安全产品

漏洞描述

OpenSSH存在远程代码执行漏洞（CVE-2024-6387）

OpenSSH 是一套用于安全访问和管理远程计算机的工具，基于 SSH 协议提供加密通讯。OpenSSH 包含 SSH 客户端和 SSHD 服务端，sshd 是 OpenSSH 的核心组件，负责处理来自远程计算机的连接请求，提供安全的远程登录、文件传输和隧道代理等功能。
2024 年 7 月，互联网公开披露了一个 OpenSSH 的远程代码执行漏洞（CVE-2024-6387）。鉴于该漏洞虽然利用较为困难但危害较大，建议所有使用受影响的企业尽快修复该漏洞。

01漏洞描述 Description

漏洞成因

CVE-2024-6387 是 OpenSSH 服务器中的一个严重漏洞，影响基于 glibc 的 Linux 系统。攻击者可以利用该漏洞在无需认证的情况下，通过竞态条件远程执行任意代码，获得系统控制权。这个漏洞源于处理超时信号时的不安全操作，最早在 OpenSSH 8.5p1 版本中引入。

漏洞影响

成功利用该漏洞的攻击者可以以 root 身份进行未经身份验证的远程代码执行 (RCE)
在某些特定版本的 32 位操作系统上，攻击者**最短**需 6-8 小时即可获得最高权限的 root shell。而在 64 位机器上，目前没有在可接受时间内的利用方案，但未来的改进可能使其成为现实。

处置优先级：高

漏洞类型：远程代码执行

漏洞危害等级：高

触发方式：网络远程

权限认证要求：无需权限

系统配置要求：默认配置可利用

用户交互要求：无需用户交互

利用成熟度：部分 EXP 已公开（适配单一版本，32 位系统）

批量可利用性：可使用通用原理 POC/EXP 进行检测/利用

修复复杂度：中，官方提供升级修复方案

02影响版本 Affects

8.5p1 <= OpenSSH < 9.8p1

03解决方案 Solution

临时缓解方案

如果暂时无法更新或重新编译 sshd
1. 可以在配置文件中将 LoginGraceTime 设置为 0（永不超时）。这样虽然会使 sshd 暴露于拒绝服务攻击（占满所有 Startups 连接），但可以避免远程代码执行风险。
2. 启用 fail2ban 等防护机制，封禁发生过多次失败登录 ssh 尝试的来源 IP。

升级修复方案

将 OpenSSH 更新到最新版本 9.8 或者各发行版本的修复版本。

漏洞解决方案

防火墙FW、入侵检测IPS、负载均衡LB Comware V5 V7 V9都不涉及该漏洞。