网络安全预警通报

2024 年第 5 期 （总第 48 期）

西安交通大学网络信息中心 2024 年 7 月 2 日

【预警类型】高危预警

【预警内容】

OpenSSH 远程代码执行漏洞(CVE-2024-6387)安全风险通告

漏洞编号：QVD-2024-24908,CVE-2024-6387

一、漏洞概述

OpenSSH 是一套基于安全外壳（SSH）协议的安全网络实用程序，它可提供加密功能保护隐私和文件传输的安全，使其成为远程服务器管理和安全数据通信的首选工具。

近日，监测发现 OpenSSH 修复了一个远程代码执行漏洞(CVE-2024-6387)，该漏洞是由于 OpenSSH 服务器(sshd)中的信号处理程序竞争问题导致，未经身份验证的攻击者可以利用此漏洞在 Linux 系统上以 root 身份执行任意代码，目前该漏洞技术细节（含 PoC）已在互联网上公开。且有近千万个 OpenSSH 实例在互联网公开，建议受漏洞影响的用户及时升级至最新版本修复该漏洞，或采用安全防护措施加强防护能力，防范网络攻击。

二、漏洞详情

综合各方信息和初步验证结果，尽管攻击者基于已公开 PoC 在开启地址分布随机化（ASLR）的环境中需要 6～8 小时的时间才能攻击成功，且可能伴有内存破坏的后果，但并不能据此得出这是一个难以致效的漏洞的结论。防御时间窗口价值仅对具备有效防护管理的资产才是有效的，快速实施加固配置和修复漏洞依然是很大的挑战。由于攻击者具有选择目标和攻击时间窗口的主动权，且掌握大量僵尸/跳板节点资源，其可以基于大量长时间并发连接，“捞取”缺乏有效防护管理的突破节点。对这些防御管理缺失的资产来说，平均 6～8 小时的攻击作业时间窗口带来的防御价值，几乎可以忽略不计。

该攻击可能被用于扩展僵尸网络、挖矿等攻击活动，同时也会在无管理目标网络中，被 APT 攻击者用于突防和内部横向移动。与此同时，我们还需要警惕漏洞可用性的演进，包括可能和其他组合利用。包括该漏洞利用是否本身存在某种高阶形态。从安全管理、监测角度，可以肯定近期会有相关端口服务的流量连接增加，监测相关流量和连接、关注内存崩溃事件和日志，并可以采取关闭不需要开放的相关端口（默认 22）服务、联动封堵可疑访问 IP、定时 Reset 超长时间连接、对于设备或服务器的管理设定访问 IP 或范围限制等方式进行防护。

漏洞影响范围：

OpenSSH < 4.4p1

8.5p1 <= OpenSSH < 9.8p1

三、处置建议

目前官网已发布最新安全版本修复此漏洞，建议受影响用户升级至以下安全版本。

OpenSSH > 9.8p1

四、漏洞缓解措施

在无法通过补丁修复的情况下，可使用以下方式进行缓解。

1．检查并启用加固措施：确保已经开启了内存地址空间布局随机化（ASLR）。

2．设置用户访问策略，只给受信任的用户授权 SSH 登录权限。

3．对系统或主机启用双因素身份验证（2FA）。

目前有提出在配置文件中将 LoginGraceTime 设置为 0 的方式来缓解该 RCE 风险的建议，但这种方法容易使 sshd 受到拒绝服务攻击，需要防御者根据自身的场景条件决定，开启该方法会增加服务器的连接占用，用于主机管理、设备管理、服务管理等低频的专用服务场景，特别是内网节点防范横向移动等可以采取此措施；但依托 OpenSSH 支撑开放的服务，需要慎重考虑是否采用该方法。