网络安全预警通报

2026 年第 1 期（总第 59 期）

西安交通大学网络信息中心 2026 年 01 月 26 日

【预警类型】高危预警

【预警内容】

GNU InetUtils telnetd 远程认证绕过漏洞（CVE-2026-24061）高危利用风险通报

一、漏洞概述

安全研究人员近日披露 GNU InetUtils 组件中的 telnetd 服务存在严重远程认证绕过漏洞，漏洞编号为 CVE-2026-24061。该漏洞源于 telnetd 在调用/usr/bin/login 进行用户认证时，未对用户可控的环境变量进行有效校验，攻击者可通过构造恶意环境变量参数，绕过正常的密码校验流程。

在漏洞被成功利用的情况下，攻击者无需合法账号或密码，即可直接获取 root 权限，从而完全控制目标服务器。由于 telnetd 通常以高权限运行，漏洞一旦被利用，可能导致服务器被接管、数据被篡改或进一步作为跳板实施横向攻击，安全风险极高。

目前该漏洞的 PoC/EXP 已在互联网上公开，且漏洞利用复杂度低，攻击门槛较低，建议相关用户立即开展排查与处置工作，避免业务系统受到影响。

二、漏洞详情

1.技术原理

漏洞类型：远程认证绕过

漏洞等级：严重

产生原因：

GNU InetUtils 中的 telnetd 服务在处理远程 Telnet 连接时，会调用系统/usr/bin/login 程序完成用户身份认证。但在该调用过程中，telnetd 未对部分传入的环境变量参数进行安全校验，攻击者可通过构造特定的环境变量值，影响 login 的认证逻辑。

在特定条件下，攻击者可绕过密码验证流程，直接获得 root 权限，进而对系统进行任意操作。该漏洞不依赖复杂交互，仅需建立 Telnet 连接并发送构造好的参数即可触发。

2.利用条件

- 目标系统启用了 telnet 服务（telnetd 正在运行）
- 使用受影响版本的 GNU InetUtils
- 攻击者可通过网络访问 telnet 服务端口

关联风险：

- 服务器 root 权限被直接获取
- 系统数据被窃取或破坏

- 作为攻击跳板发起进一步内网攻击

三、漏洞影响范围

1. 受影响版本

GNU InetUtils：1.9.3≤版本≤2.7

2. 受影响系统

Debian 12

Debian 13

Ubuntu 24.04 及以上版本

Kali Linux

部分 NAS 存储系统

3.威胁严重性

CVSS v3.x 评分为 9.8（Critical）。

鉴于该漏洞可实现远程认证绕过并直接获取 root 权限，且 PoC 已公开，整体风险需按最高级别进行处置。

四、处置建议

1.立即将 GNU InetUtils 升级至官方最新版本或 2.7 以上安全版本。

2.非必要场景下，建议直接禁用 telnet 服务，使用 SSH 等安全替代方案。

3.如无法立即升级，建议自定义 login 工具并禁用-f 参数，降低被利用风险。