网络安全预警通报

2026 年第 4 期（总第 62 期）

西安交通大学网络信息中心 2026 年 05 月 07 日

【预警类型】高危预警

【预警内容】

Android 无线 ADB 认证绕过漏洞（CVE-2026-0073）零点击远程代码执行高危风险通报

一、漏洞概述

近期，业界披露了 Android 系统中一个严重的高危漏洞（CVE-2026-0073）。该漏洞存在于 Android 系统的 adbd(Android Debug Bridge daemon，安卓调试桥守护进程）组件中，源于 adbd_tls_verify_cert 函数的认证逻辑错误。攻击者只需与目标设备连接在同一 Wi-Fi 网络下，无需用户任何点击或交互（零点击），即可远程获取设备的 Shell 权限。一旦获取 Shell 权限，攻击者可以读取文件、窃取数据、执行系统命令并安装恶意软件，从而导致受害者个人隐私全面泄露，设备被完全控制。

该漏洞影响当前主流的 Android 14、15、16 及 16-QPR2 等多个版本。目前谷歌已于 2026 年 5 月安全更新中修复此漏洞。考虑到攻击条件极易达成，建议各单位及个人用户立即开展排查和修复工作。

二、漏洞详情

1.技术原理

漏洞编号：CVE-2026-0073

漏洞名称：Android adbd TLS 证书校验绕过

漏洞类型：认证绕过→零点击远程代码执行（RCE）

漏洞等级：高危

公开日期：2026 年 5 月 4 日

CVSS 评分：8.8

产生原因：

在无线 ADB 的双向认证过程中，auth.cpp 文件中的 adbd_tls_verify_cert 函数未能正确验证客户端证书。攻击者可构造恶意的 TLS 握手包，绕过证书校验，直接与 adbd 建立连接并获取 Shell 权限。整个过程无需用户点击授权弹窗，属于典型的“零点击”攻击。

2.利用条件

- 攻击者与目标设备连接在同一局域网（如同一 Wi-Fi 热点或同网段）
- 目标设备系统版本为 Android 14/15/16/16-QPR2
- 目标设备安全补丁级别早于 2026 年 5 月 1 日
- 目标设备开启了“无线调试”功能（开发者选项中：默认关闭，但若开启则风险极高）

三、漏洞影响范围

1.受影响版本

Android 系统版本范围：Android 14～Android 16-QPR2

具体包括但不限于：

Android 14（安全补丁早于 2026-05-01）

Android 15（安全补丁早于 2026-05-01）

Android 16（安全补丁早于 2026-05-01）

Android 16-QPR2（安全补丁早于 2026-05-01）

注：Android 13 及更早版本已停止官方技术支持，不在受影响范围内。

2.威胁严重性

该漏洞可实现零点击远程代码执行，攻击者仅需与目标同处一个 Wi-Fi 网络即可稳定利用，无需用户任何交互。一旦成功，攻击者可获取 Shell 权限，进而导致隐私全面泄露（通讯录/短信/相册/定位等）、沙箱逃逸（跨应用窃取数据）、持久化控机（植入远控木马）。公共 Wi-Fi 场景（商场、酒店、机场、校园公共区域）风险尤为突出。综合评估为高危，建议按最高优先级进行应急处置。

四、处置建议

1.官方修复方案（推荐）

将 Android 设备的安全补丁级别更新至 2026 年 5 月 1 日或之后。