网络安全预警通报

2025 年第 4 期 （总第 54 期）

西安交通大学网络信息中心 2025 年 4 月 11 日

【预警类型】高危预警

【预警内容】

“DeepSeek”仿冒 AI 工具传播木马病毒紧急风险通告

一、漏洞概述

近日，国家计算机病毒协同分析平台发现一款伪装为人工智能工具“DeepSeek”的新型手机木马病毒在我国境内传播。该病毒通过仿冒“DeepSeek”官方 App 进行传播，一旦用户在安卓设备上点击运行，即会诱导进行“更新”操作，从而安装恶意子程序，进一步窃取用户隐私数据，并可能用于电信网络诈骗。

此外，还发现多个伪造的“DeepSeek.exe”“DeepSeek.msi”“DeepSeek.dmg”病毒文件，攻击者试图通过伪造 DeepSeek 尚未推出的 Windows 与 Mac 客户端扩展攻击范围。

二、漏洞详情

1.技术原理

漏洞类型：仿冒应用传播的木马病毒。

攻击路径：攻击者通过仿冒“DeepSeek”App，诱导用户下载安装，获取高权限后窃取用户隐私数据。

2.利用条件

必要条件：用户下载并安装了伪造的“DeepSeek”应用程序。

关联风险：攻击者可能借助用户数据发动电信诈骗，冒用用户身份向联系人发送诈骗信息。

三、漏洞影响范围

1.受影响的操作系统：

Android 系统

Windows 系统

MacOS 系统

2.受影响的文件：

DeepSeek.apk

DeepSeek.exe

DeepSeek.msi

DeepSeek.dmg

特别提醒：截至目前 2025 年 4 月 11 日 DeepSeek 官方仅提供网页版服务，未授权任何第三方发布移动端或桌面端应用程序。任何以安装包形式传播的“DeepSeek”客户端程序均可判定为恶意伪装。

四、处置建议

1.应用来源核实：严禁通过短信、二维码、网盘、社交软件等非正规渠道安装 DeepSeek App。DeepSeek 目前仅提供网页版服务；

2.安全软件实时开启：启用预装或第三方安全软件，并及时更新病毒库；

3.权限审核：拒绝任何未知应用申请的后台运行、无障碍、设备管理等高权限；

4.可疑文件检测：可将下载文件上传至国家病毒平台进行检测；https://virus.cverc.org.cn/#/entirety/upload

5.设备安全处置：若疑似中招，应在专业人员指导下完成通讯录备份与系统恢复，并留意账户是否存在异常登录。

五、附录

建议仅通过官网访问使用 https://www.deepseek.com/

国家计算机病毒协同分析平台：

https://virus.cverc.org.cn/#/entirety/upload