网络安全预警通报

2025 年第 5 期 （总第 55 期）

西安交通大学网络信息中心 2025 年 4 月 21 日

【预警类型】高危预警

【预警内容】

关于 WinRAR 解压软件存在高危漏洞风险的通报

一、漏洞概述

近日，日本安全团队 CSIRT 披露了 WinRAR 压缩软件中的一项安全漏洞（CVE-2025-31334）。该漏洞可被攻击者利用来绕过 Windows 系统的 Mark of the Web（MoTW）安全机制，从而在用户打开压缩包内容时，悄无声息地执行恶意代码，而不会弹出 Windows 系统的安全警告提示。

MoTW 机制通常用于提醒用户警惕来自网络的可疑文件，而该漏洞可直接绕过该机制，大幅提升了木马、病毒传播的隐蔽性和成功率。攻击者可通过发送含有特殊构造的压缩包诱导用户打开，在无需用户进一步确认的前提下执行后门程序、信息窃取木马等恶意代码，严重威胁终端系统与用户数据安全。

二、漏洞详情

1.技术原理

漏洞类型：安全机制绕过漏洞

攻击路径：攻击者构造特定格式的 WinRAR 压缩包，植入指向恶意可执行文件的符号链接，当用户解压后运行，Windows 系统不会弹出 MoTW 安全警告，直接执行恶意程序。

2.利用条件

必要条件：用户使用了存在漏洞的旧版本 WinRAR（低于 7.11），并手动打开了来自网络的不明压缩包内容。

关联风险：攻击者可在无用户感知情况下执行恶意程序，实现远程控制、数据窃取、勒索等攻击行为。

三、漏洞影响范围

1.受影响的 WinRAR 版本

WinRAR 7.11 版本以前的所有版本均受影响。

2.受影响平台

Windows 系统

特别提醒：WinRAR 作为使用广泛的压缩工具，在教育、科研、办公终端中大量部署，需高度警惕并及时完成版本更新。

四、处置建议

1.立即升级 WinRAR 版本：建议各单位尽快到 WinRAR 官网升级至最新版本 7.11 或以上版本。

2.清查旧版软件：通过资产管理系统或手动方式排查并卸载所有旧版 WinRAR 客户端，防止被恶意利用。

3.强化用户安全意识：请勿随意打开来源不明的压缩包文件，尤其是通过邮件、论坛、社交平台等途径获取的可执行文件。