网络安全预警通报

2024 年第 7 期 （总第 50 期）

西安交通大学网络信息中心 2024 年 8 月 9 日

【预警类型】高危预警

【预警内容】

Windows 远程桌面授权服务远程代码执行漏洞

漏洞编号：CVE-2024-38077

一、漏洞概述

今日，监测到微软披露 Windows 操作系统最新超高危漏洞，漏洞编号：CVE-2024-38077，漏洞危害等级：严重。漏洞特点：攻击复杂性低、可稳定利用、受影响范围广、破坏力大。

二、漏洞详情

远程代码执行漏洞存在于 Windows 远程桌面许可管理服务（RDL）中，该服务被广泛部署于开启 Windows 远程桌面（3389 端口）的服务器，用于管理远程桌面连接许可。

该漏洞允许未经身份验证的远程攻击者在受影响的系统上执行任意代码，是由 Windows 远程桌面授权服务中的基于堆的缓冲区溢出引起的。通过该漏洞，攻击者只须针对开启了相关服务的服务器发送特制数据包，即可完全控制目标系统，获得最高的 SYSTEM 权限。

三、漏洞危害

攻击者可以通过发送特制的请求到受影响的服务来利用此漏洞完全控制系统。

四、漏洞影响范围

该漏洞影响范围广泛，涉及 Windows 2000 后所有开启远程桌面的 Windows 服务器操作系统即 Windows Server 2000 - Windows Server 2025

五、漏洞处置建议

目前，厂商已发布补丁修复漏洞，建议相关用户及时确认是否受到漏洞影响，尽快更新至安全版本。