安全通告

关于 Windows 远程桌面授权服务存在远程代码执行漏洞的预警通报

发布日期：2024-8-9

[2024]019 号

漏洞描述

2024 年 8 月 9 日监测发现 Windows 远程桌面授权服务中存在堆缓冲区溢出漏洞（CVE-2024-38077），该漏洞是因为 RD Licensing Server 未能正确处理特制的 RDP 协议流量，允许未经身份验证的威胁者可以连接到远程桌面授权服务并发送恶意消息，成功利用可能导致远程代码执行。

Windows Remote Desktop Licensing Service(RDS Licensing Service)是 Windows Server 中的一个服务，它负责管理和分发远程桌面服务的客户端访问许可证（CALs）。要使用远程桌面服务，用户和组织需要购买并安装相应的客户端访问许可证（CALs）。这些许可证允许用户从远程位置访问服务器上的资源。

漏洞编号

CVE-2024-38077

漏洞危害

未经身份验证的攻击者利用这一漏洞可以向设置为远程桌面授权服务器的服务器发送特制的数据包，触发缓冲区溢出从而在目标系统上执行任意代码。

漏洞等级

高危

受影响版本

Windows Server 2000 - Windows Server 2025

修复方案

微软官方已发布补丁公告，建议受影响用户安装该漏洞的安全更新，即时计划禁用远程桌面授权服务。

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38077

参考链接

https://www.cve.org/CVERecord?id=CVE-2024-38077