关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告

转载自：
https://www.cert.org.cn/publish/main/9/2019/20190515134947228198452/20190515134947228198452_.html

2019 年 5 月 15 日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft 远程桌面服务远程代码执行漏洞（CNVD-2019-14264）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞细节虽未公开，但已引起社会高度关注，微软公司已发布官方补丁。

一、漏洞情况分析

MicrosoftWindows 是美国微软公司发布的视窗操作系统。远程桌面连接是微软从 Windows 2000 Server 开始提供的组件。

2019 年 5 月 14 日，微软发布了本月安全更新补丁，其中修复了远程桌面协议（RDP）远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，向目标 Windows 主机发送恶意构造请求，可以在目标系统上执行任意代码。由于该漏洞存在于 RDP 协议的预身份验证阶段，因此漏洞利用无需进行用户交互操作。该漏洞存在被不法分子利用进行蠕虫攻击的可能。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响的产品版本包括：

Windows 7 for 32-bit Systems Service Pack 1

Windows 7 for x64-based Systems ServicePack 1

Windows Server 2008 for 32-bit SystemsService Pack 2

Windows Server 2008 for 32-bit SystemsService Pack 2 (Server Core installation)

Windows Server 2008 for Itanium-BasedSystems Service Pack 2

Windows Server 2008 for x64-based SystemsService Pack 2

Windows Server 2008 for x64-based SystemsService Pack 2 (Server Core installation)

Windows Server 2008 R2 for Itanium-BasedSystems Service Pack 1

Windows Server 2008 R2 for x64-basedSystems Service Pack 1

Windows Server 2008 R2 for x64-basedSystems Service Pack 1 (Server Core installation)

Windows XP SP3 x86

Windows XP SP2 x64

Windows XP Embedded SP3 x86

Windows Server 2003 SP2 x86

Windows Server 2003 SP2 x64

CNVD 秘书处组织技术支撑单位对 RDP 服务在全球范围内的分布情况进行分析，结果显示该服务的全球用户规模约为 939.0 万，其中位于我国境内的用户规模约为 193.0 万。

三、漏洞处置建议

目前，微软官方已发布补丁修复此漏洞，CNVD 建议用户立即升级至最新版本：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

另可采取下列临时防护措施：

1、禁用远程桌面服务。

2、通过主机防火墙对远程桌面服务端口进行阻断（默认为 TCP 3389）。

3、启用网络级认证（NLA），此方案适用于 Windows 7、Windows Server 2008 和 Windows Server 2008 R2。启用 NLA 后，攻击者首先需要使用目标系统上的有效帐户对远程桌面服务进行身份验证，然后才能利用此漏洞。

附：参考链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/