

2019年5月15日

# 河南省教育信息安全监测中心

# RDP远程代码执行漏洞预警

# Microsoft RDP远程代码执行漏洞预警

**事件描述**

2019年5月15日，河南省教育信息安全监测中心在针对教育行业的Web应用进行安全监测时，发现互联网存在Microsoft Windows Remote Desktop Services漏洞公告，该公告表示Microsoft Windows Remote Desktop Services存在远程代码执行漏洞，经检测，大量用户受到该类漏洞的影响。

Remote Desktop Services远程桌面服务，是Windows操作系统自带的一项服务。2019年5月15日，研究人员发现Microsoft Windows从XP到2008 R2多个版本Remote Desktop Services远程代码执行漏洞，经河南省教育信息安全监测中心研判，该漏洞可能严重影响广大教育用户的信息业务系统。

远程桌面服务（以前称为终端服务）中存在远程代码执行漏洞，未经身份验证的攻击者可以使用RDP连接到目标系统并发送精心设计的请求。此漏洞是预身份验证，不需要用户交互。成功利用此漏洞的攻击者可以在目标系统上执行任意代码。然后，攻击者可以安装程序；查看、更改或删除数据；或者创建具有完全用户权限的新帐户。

**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

**处置建议**

目前，微软官方已发布补丁修复此漏洞，河南省教育信息安全监测中心建议广大教育行业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/>

**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/>