河南省教育信息安全监测中心

Windows Print Spooler CVE-2021-1675 及 CVE-2021-34527 远程代码执行漏洞预警

2021 年 7 月 7 日

Windows Print Spooler（CVE-2021-34527）（CVE-2021-1675）远程代码执行漏洞预警

一、事件描述

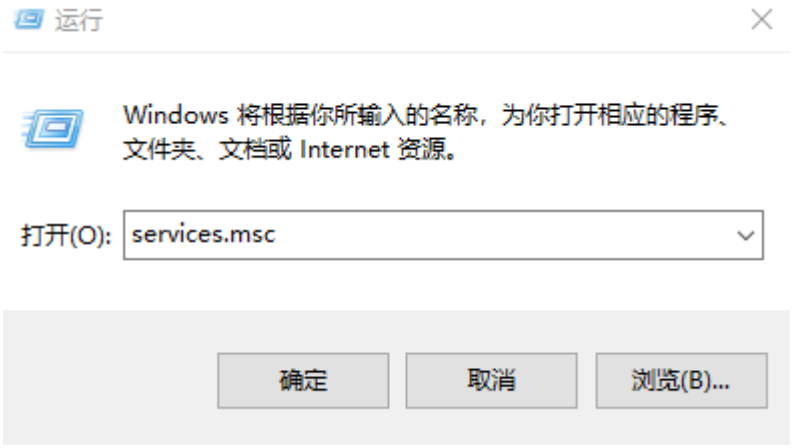
近日，网络安全威胁和漏洞信息共享平台发布漏洞预警，公布了微软 Windows Print Spooler 远程代码执行漏洞的风险公告，漏洞 CVE 编号：CVE-2021-1675 和 CVE-2021-34527，根据公告，攻击者只需一个普通权限的用户，即可对目标网络中的 Windows 系统发起远程攻击，控制存在漏洞的域控制器、服务器和 PC，从而控制整个网络。该漏洞广泛的存在于各个版本的 Windows 操作系统中，利用难度和复杂度低，危害极大。目前暂无相关补丁。

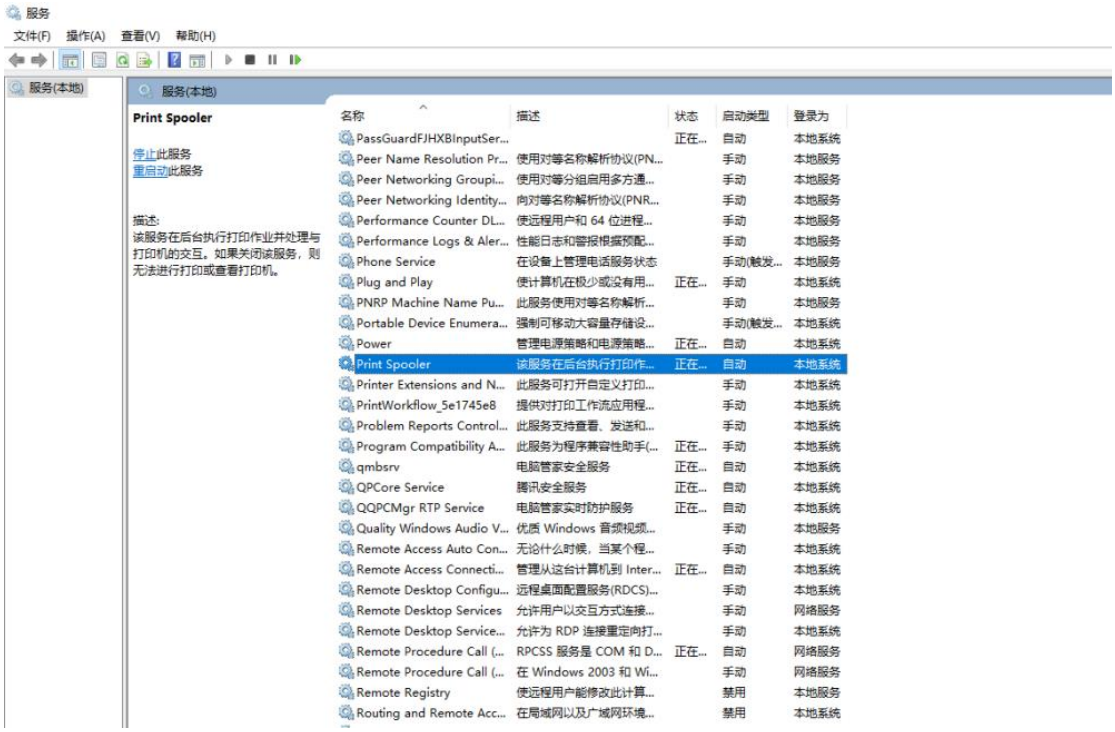
二、安全暂时处置建议

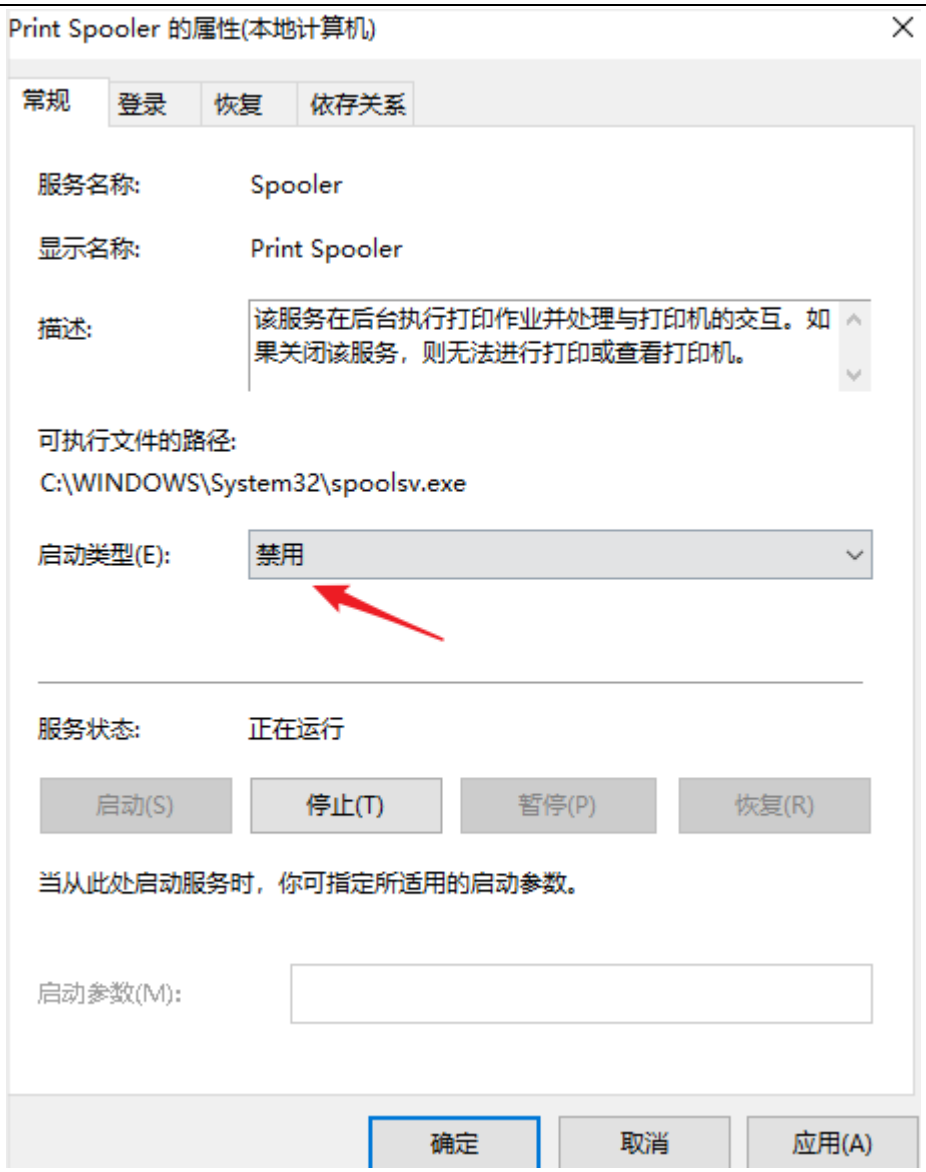
请首先确定 Print Spooler 服务是否正在运行，如果 Print Spooler 正在运行或该服务未设置为禁用，以下两个暂时性的解决方案可任选其一：

1、对于未启用安全域管理的终端用户。建议禁用 Windows Print Spooler 服务，但这会导致打印服务不可用，建议需要打印时临时开启服务，用完禁止该服务，等待漏洞补丁发布。具体操作：

在“windows 管理工具->服务”中，禁用“Print Spooler”或通过命令输入：“services.msc”。如下图所示操作：




服务
文件(F) 操作(A) 查看(V) 帮助(H)
服务(本地)
服务(本地)
Print Spooler
停止此服务
重启动此服务
描述:
该服务在后台执行打印作业并处理与打印机的交互。如果关闭该服务，则无法进行打印或查看打印机。
名称 描述 状态 启动类型 登录为
PassGuardFJHXBInputSer... 正在... 自动 本地系统
Peer Name Resolution Pr... 使用对等名称解析协议(PN... 手动 本地服务
Peer Networking Groupi... 使用对等分组启用多方通... 手动 本地服务
Peer Networking Identity... 向对等名称解析协议(PNR... 手动 本地服务
Performance Counter DL... 使远程用户和 64 位进程... 手动 本地服务
Performance Logs & Aler... 性能日志和警报根据预配... 手动 本地服务
Phone Service 在设备上管理电话服务状态 手动(触发... 本地服务
Plug and Play 使计算机在极少或没有用... 正在... 手动 本地系统
PNRP Machine Name Pu... 此服务使用对等名称解析... 手动 本地服务
Portable Device Enumera... 强制可移动大容量存储设... 手动(触发... 本地系统
Power 管理电源策略和电源策略... 正在... 自动 本地系统
Print Spooler 该服务在后台执行打印作... 正在... 自动 本地系统
Printer Extensions and N... 此服务可打开自定义打印... 手动 本地系统
PrintWorkflow_5e1745e8 提供对打印工作流应用程... 手动 本地系统
Problem Reports Control... 此服务支持查看、发送和... 手动 本地系统
Program Compatibility A... 此服务为程序兼容性助手(... 正在... 手动 本地系统
qmbsrv 电脑管家安全服务 正在... 自动 本地系统
QPCore Service 腾讯安全服务 正在... 自动 本地系统
QQPCMgr RTP Service 电脑管家实时防护服务 正在... 自动 本地系统
Quality Windows Audio V... 优质 Windows 音频视频... 手动 本地服务
Remote Access Auto Con... 无论什么时候，当某个程... 手动 本地系统
Remote Access Connecti... 管理从这台计算机到 Inter... 正在... 自动 本地系统
Remote Desktop Configu... 远程桌面配置服务(RDCS)... 手动 本地系统
Remote Desktop Services 允许用户以交互方式连接... 手动 网络服务
Remote Desktop Service... 允许为 RDP 连接重定向打... 手动 本地系统
Remote Procedure Call (... RPCSS 服务是 COM 和 D... 正在... 自动 网络服务
Remote Procedure Call (... 在 Windows 2003 和 Wi... 手动 网络服务
Remote Registry 使远程用户能修改此计算... 禁用 本地服务
Routing and Remote Acc... 在局域网以及广域网环境... 禁用 本地系统



对于使用安全域管理，操作方式如下：

1）以域管理员身份运行以下命令：

Get-Service -Name Spooler

2）如果 Print Spooler Service 正在运行或该服务未被禁用，请选择使用 PowerShell 执行以下任一选项来禁用 Print Spooler Service。

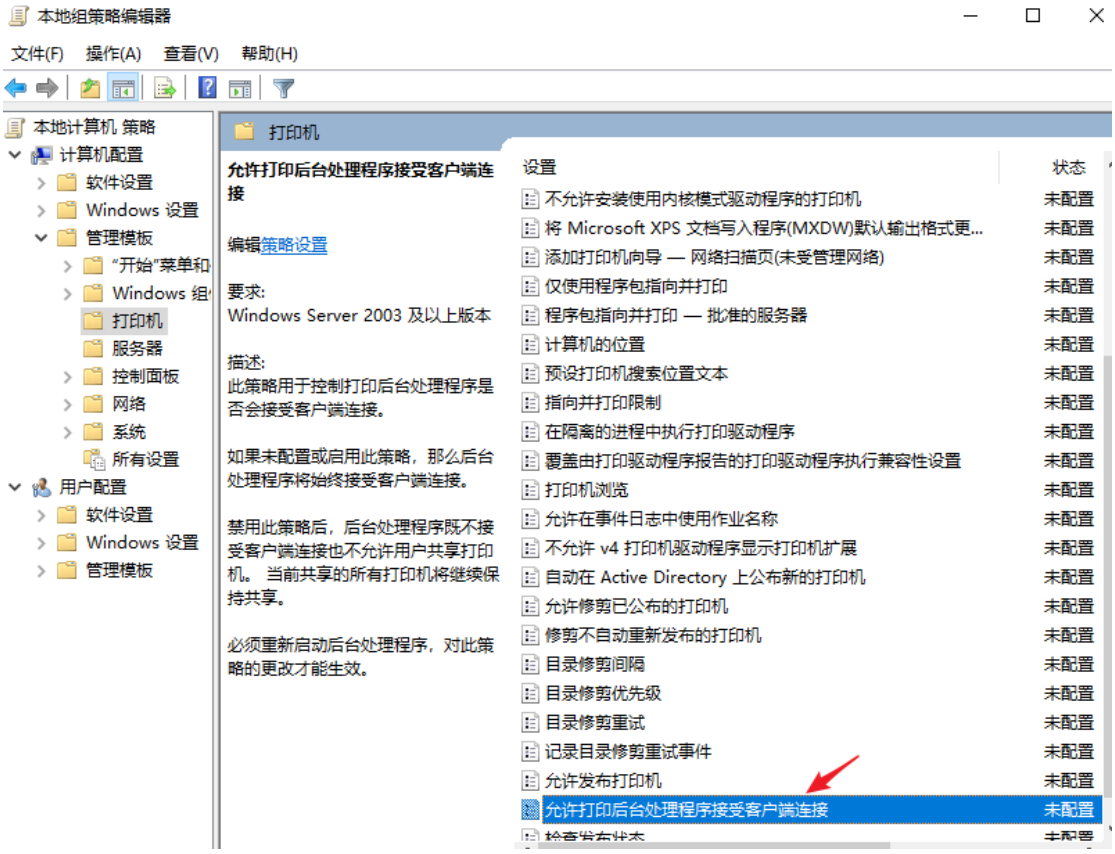
Stop-Service -Name Spooler -Force 或

Set-Service -Name Spooler -StartupType Disabled

2、通过组策略禁用入站远程打印来阻挡远程恶意攻击，但可支持本地打印服务。具体配置方法如下：

在本地组策略编辑器中，选择“计算机配置->管理模板->打印机”禁用“允

许 Print Spooler 接受客户端连接”或通过命令输入：“gpedit.msc”。如下图所示操作。



三、联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052