**附件1：终端修复策略**

用户接到通知后，请按下列方式进行处理，此方案适应所有的Windows操作系统用户。

**1、漏洞检测**

建议用户通过漏洞检测工具对网络中的漏洞威胁进行排查。下载360安全大脑进行漏洞检测，下载链接：https://www.360.cn/brain\_of\_security/。

**2、修改个人注册表，禁止SMB的压缩功能**

个人用户可通过手动修改注册表，防止被黑客远程攻击。运行regedit.exe，打开注册表编辑器，在HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Par
ameters建立一个名为DisableCompression的DWORD，值为1，禁止SMB的压缩功能。取消方法：在HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters建立一个名为DisableCompression的DWORD，值为0。

通过PowerShell命令禁用SMBv3压缩功能，执行命令为：Set-ItemProperty -Path"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force取消方法： Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServe
r\Parameters" DisableCompression -Type DWORD -Value 0 –Force。

**3、手工更新微软最新补丁**

微软目前已发布针对此漏洞的安全更新补丁：

（1）用户访问微软的官方网站，在“更新和安全性”>“ Windows Update”中检查更新来下载并安装重要的安全更新。(正版操作系统使用此规则)

（2）自行下载补丁更新

下载地址：

<https://www.catalog.update.microsoft.com/Search.aspx?q=KB4551762>

**4.修改Windows防火墙**

对于不需启用SMB 共享的 Windows 客户端和服务器，可以使用 Windows防火墙阻止所有入站 SMB 流量，以防止来自恶意或受损设备的远程连接。 在 Windows防火墙中，对以下入站规则开启禁用：文件和打印机共享 (SMB-In)，Netlogon 服务 (NP-In)，远程事件日志管理 (NP-In)，远程服务管理 (NP-In)。