中共湖南省委网络安全和信息化委员会办公室

关于对 SMBv3.0 服务远程代码执行漏洞进行预警通报的通知

各省直单位、市州委网信办:

3 月 12 日，中央网信办网络安全应急协调联动平台下发预警通报称：10 日，微软官方发布了针对 Windows 10/Server 禁用 SMBv3（SMB 3.1.1 版本）协议压缩的指南公告，以此缓解 SMBv3 协议（用于文件共享与打印服务）在处理调用请求时的一个远程代码执行漏洞（漏洞编号 CVE-2020-0796）。该漏洞的主要影响目标是 Win10 系统，其原理与“永恒之蓝”类似，存在被蠕虫化利用的可能，一旦利用成功可在目标机器上执行任意代码，潜在威胁较大。请各单位高度重视，及时采取应对措施加强防范。

一、漏洞影响范围

Windows 10 Version 1903 for 32-bit Systems

Windows 10 Version 1903 for ARM64-based Systems

Windows 10 Version 1903 for x64-based Systems

Windows 10 Version 1909 for 32-bit Systems

Windows 10 Version 1909 for ARM64-based Systems

Windows 10 Version 1909 for x64-based Systems

Windows Server, version 1903 (Server Core installation)

Windows Server, version 1909 (Server Core installation)

二、建议应对措施

1.目前微软尚未发布漏洞详情及补丁，其提供的临时缓解措施如下：

通过PowerShell命令禁用SMBv3压缩功能（是否使用需要结合业务进行判断），以阻止未经身份验证的恶意攻击者对SMBv3服务端的漏洞利用：Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force，执行此操作无需重启系统，但对SMBv3客户端无效。

取消禁用可以执行以下命令：Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 0 -Force

2.若无业务必要，在网络安全域边界防火墙封堵文件打印和共享端口（tcp:135/139/445）；

3.提醒全员保持良好办公习惯，不接收和点击来历不明的文件、邮件附件，并做好数据备份工作，防止感染病毒；

4.关注微软官方公告，及时升级官方补丁。

中共湖南省委网络安全
和信息化委员会办公室
2020年3月13日