中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）
地址：湖南省长沙市芙蓉区和光路 102 号
电话：0731-84733342　传真：0731--84783398
网址：www.cctec.org.cn

编号：TG_CCTEC202006

网络安全威胁通告

---关于 SMBv3 远程代码执行漏洞安全威胁通告（CVE-2020-0796）

服务器信息块协议（SMB 协议，Server Message Block Protocol）为网络计算机客户程序提供一种从服务程序读写文件并请求服务的方法。服务器信息块协议（SMB 协议，Server Message Block Protocol）为网络计算机客户程序提供一种从服务程序读写文件并请求服务的方法。

漏洞详情：2020 年 3 月 11 日，海外厂家发布安全规则通告，通告中描述了一处微软 SMBv3 协议的内存破坏漏洞，编号 CVE-2020-0796，并表示该漏洞无需授权验证即可被远程利用，可能形成蠕虫级漏洞。

漏洞风险：Microsoft Server Message Block 3.1.1(SMBv3)协议在处理某些请求的方式中存在代码执行漏洞，未经身份验证的攻击者发送精心构造的数据包进行攻击，可在目标 SMB 服务器上执行任意代码。

风险等级：高风险。

影响版本：

Windows 10 版本 1903（用于 32 位系统）

Windows 10 版本 1903（用于基于 ARM64 的系统）

Windows 10 版本 1903（用于基于 x64 的系统）

Windows 10 版本 1909（用于 32 位系统）

Windows 10 版本 1909（用于基于 ARM64 的系统）

Windows 10 版本 1909（用于）基于 x64 的系统

Windows Server 1903 版（服务器核心安装）

Windows Server 1909 版（服务器核心安装）

漏洞验证：POC/EXP

修复建议：

1. 微软已经发布了此漏洞的安全补丁，访问如下链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796，及时更新补丁。
2. 个人用户也可直接运行 Windows 更新，完成补丁的安装。操作步骤：设置->更新和安全->Windows 更新，点击“检查更新”。
3. 个人用户也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\Parameters 建立一个名为 DisableCompression 的 DWORD，值为 1，禁止 SMB 的压缩功能，或者关闭 445 端口，是否使用需要结合自己业务进行判断。

中国信息安全测评中心华中测评中心

（湖南省信息安全测评中心）

事业一部

2020 年 3 月 13 日