中共天津市委网络安全和信息化委员会办公室

关于 Microsoft Windows SMBv3 存在远程代码执行漏洞的预警通知

各相关单位:

近日，国家信息安全漏洞共享平台（CNVD）官方收录了 Microsoft Windows SMBv3 存在远程代码执行漏洞 （CNVD-2020-16676），攻击者可利用该漏洞远程执行代码。目前微软厂商已经发布补丁，鉴于此危害较大，且已引起社会广泛关注，建议尽快修复。

一、漏洞情况分析

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。

本次收录的 Microsoft Windows SMBv3 存在远程代码执行漏洞（CNVD-2020-16676），该漏洞为 Microsoft SMBv3 网络通信协议中的预身份验证远程代码执行漏洞。SMBv3 在处理特定请求时，存在远程代码执行漏洞，该漏洞影响 SMBv3 服务器和 SMBv3 客户端。未经身份验证的攻击者可通过向受影响 SMBv3 服务器发送特制的压缩数据包来利用此漏洞，攻击者还可以通过配置恶意 SMBv3 服务器并诱导用户连接来利用此漏洞，成功利用此漏洞的远程攻击者可在目标

机器上执行任意代码。值得注意的是，此漏洞存在客户端访问恶意服务端的利用场景，所以理论上引入了浏览器的攻击面。

微软官方将此漏洞标记为“被利用可能性高”。截至目前，此漏洞已经被修复并分配 CVE 编号为 CVE-2020-0796，同时官方已发布修复补丁建议，请各单位自查，并尽快修复升级至最新版本。

CNVD 对该漏洞的综合评级为“高”。

二、漏洞影响范围

Windows 10 Version 1903 for 32-bit Systems

Windows 10 Version 1903 for x64-based Systems

Windows 10 Version 1903 for ARM64-based Systems

Windows Server, Version 1903 (Server Core installation)

Windows 10 Version 1909 for 32-bit Systems

Windows 10 Version 1909 for x64-based Systems

Windows 10 Version 1909 for ARM64-based Systems

Windows Server, Version 1909 (Server Core installation)

三、漏洞处置建议

目前，微软官方已发布针对此漏洞受影响版本的补丁程序，该安全更新通过更正 SMBv3 协议处理这些特制请求的

方式来解决此漏洞。建议用户参考以下链接尽快安装补丁程序:

https://Portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

如果暂时无法安装补丁程序，可采取临时缓解措施:

1、禁用 SMBv3 compression。

微软官方给出了缓解措施来禁用 SMBv3 compression。用户可使用以下 PowerShell 命令禁用 compression 功能，以阻止未经身份验证的攻击者利用此漏洞来攻击 SMBv3 服务器:

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force

请注意: 进行更改后，无需重新启动;此解决方法不能防止针对 SMB 客户端的利用。

使用以下 PowerShell 命令可解除禁用 compression:

Set-ItemProperty -Path "HKLM:\SYSTEM\ CurrentControlSet\Services\La nmanServer\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，不接受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。

请各单位高度重视，严格贯彻落实《党委（党组）网络安全工作责任制》要求，加强风险排查和安全防护工作，如发生重大网络安全事件及时上报市委网信办。

市委网信办

2020年3月16日