中共山西省委网络安全和信息化委员会办公室

晋网安字〔2020〕97号

关于防范 Microsoft Windows SMBv3 远程代码执行漏洞的风险提示

各市委网信办、省直各有关单位、各新闻网站：

近日，国家信息安全漏洞共享平台（CNVD）收录了 Microsoft Windows SMBv3 远程代码执行漏洞（CNVD-2020-16676，对应 CVE-2020-0796）。攻击者利用该漏洞无需权限即可实现远程执行任意代码。该漏洞的综合评级为“高危”。

一、漏洞基本情况

SMB（Server Message Block）协议作为一种局域网文件共享传输协议，常被用来作为共享文件安全传输研究的平台。由于 SMB3.1.1 协议中处理压缩消息时，对其中数据没有经过安全检查，直接使用会引发内存破坏漏洞，可能被攻击者利用远程执行任意代码，受黑客攻击的目标系统只要开机在线即可能被入侵。该漏洞原理与“永恒之蓝”类似，存在被蠕虫化利用的可能。

二、漏洞影响范围

此次漏洞影响范围较广，凡在网络中使用 Windows 10 1903 版本之后的所有终端，如 Windows 家庭版、专业版、企业版、教育版，Windows 10 1903 （19H1）、Windows 10 1909、Windows Server 19H1 均为潜在攻击目标。

漏洞影响的产品版本包括：

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)

三、漏洞处置建议

1.若无业务必要，通过 PowerShell 命令禁用 SMBv3 压缩功能；

2.若无业务必要，暂时关闭文件打印和共享端口（tcp:135/139/445）；

3.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.目前，微软已公布补丁更新，建议各单位在确保安全的前提下，尽快下载补丁更新，避免引发相关网络安全事件。

省委网信办网络安全应急值班电话 17735162917

技术支持：国家计算机网络与信息安全管理中心山西分中心 0351-8788226

中共山西省委网信办

2020 年 3 月 17 日

办公室