河南省教育信息安全监测中心

微软 SMBv3 远程代码执行漏洞安全预警

（第二次）

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2020 年 6 月 4 日

微软 SMBv3 远程代码执行漏洞安全预警

(第二次)

事件描述

2020 年 3 月 12 日，微软官方发布了 WindowsSMBv3 客户端/服务器远程代码执行漏洞的安全更新细节和补丁程序，微软官方将此漏洞标记为“被利用可能性高”。

6 月 4 日，省教育信息安全监测中心工作人员发现，有国外安全研究员在 GitHub 上公开了一份此漏洞的远程代码执行利用代码，漏洞的现实威胁进一步升级。由于漏洞无需用户验证的特性，可能导致类似 WannaCry 攻击那样蠕虫式的传播。鉴于漏洞危害很大，再次建议教育行业用户尽快安装补丁更新。

漏洞编号

CVE-2020-0796

影响版本

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)

安全建议

一、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

二、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

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

（2）网络端口限制

在企业外围防火墙处阻止 445 端口的连接 TCP 端口 445 用于启动与受影响组件的连接。在网络外围防火墙处阻止此端口将有助于保护位于防火墙后面的系统免受尝试利用此漏洞的攻击。这可以保护网络免受来自企业外围的攻击。在企业范围内阻止受影响的端口是避免基于 Internet 的攻击的最佳防御方法。但是，系统仍可能受到企业内网络的攻击。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052