### 奇安信CVE-2020-0796检测工具使用手册

“奇安信CVE-2020-0796检测工具”是针对 Microsoft SMBv3远程代码执行漏洞“CVE-2020-0796”推出的一款远程扫描工具。该工具可以快速扫描检测内网终端是否支持SMB v3.1.1，同时检测其是否还存在“CVE-2020-0796”漏洞。

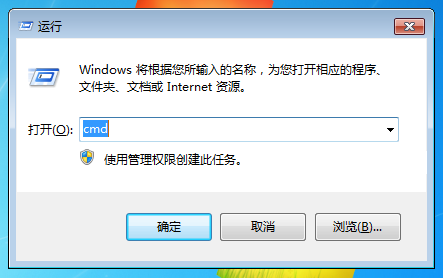
**一． 工具说明：**

支持IP段批量扫描检测局域网内终端是支持Microsoft SMBv3功能，以及支持该功能的终端是否已经修“CVE-2020-0796”漏洞。适合对局域网全网段扫描，以快速找到局域网内存在该漏洞的全部终端设备。

申明：本漏洞扫描工具仅限于网络安全管理员发现本组织的问题系统使用，依据网络安全法，任何攻击为目的对非授权系统的非法使用所导致的后果自负。

**二、使用说明：**

1. 下载文件进行解压。
2. 使用win+R快捷键或开始菜单选择“运行”，输入cmd。调起命令行工具。



1. 在命令行工具，输入：快速扫描检测工具的完整路径或将文件拖动到命令中。回车后根据提示，输入IP1-IP2（或单个IP）可以得到结果，详见如下示例：

C:\Users\qdy>C:\Users\qdy\Desktop\CVE-2020-0796-Scanner.exe

请输入目标IP或IP范围:

192.168.0.2-192.168.0.254

本漏洞扫描工具仅限于网络安全管理员发现本组织的问题系统使用，依据网络安全法，任何攻击为目的对非授权系统的非法使用所导致的后果自负。

[+] 目标 [192.168.0.1] 不支持SMB v3.1.1，或网络连接失败

[+] 目标 [192.168.0.2] 已支持SMB v3.1.1

[+] 目标 [192.168.0.2] 仍存在漏洞风险

[+] 目标 [192.168.0.3] 已支持SMB v3.1.1

[+] 目标 [192.168.0.4] 已修复漏洞

以上结果表示：

不支持SMB v3.1.1，或网络连接失败-表示没有该漏洞或无法连接该终端。

已支持SMB v3.1.1：

仍存在漏洞风险-表示支持SMB v3.1.1，并且有漏洞，需要修复。

已修复漏洞-表示支持SMB v3.1.1，并且漏洞已经修复。

**三、如何修复“CVE-2020-0796”漏洞**

如果存在“CVE-2020-0796”该漏洞建议安装奇安信天擎终端安全管理系统，使用漏洞修复功能尽快修复漏洞。或使用Windows系统自带的漏洞修复功能打补丁。

**四、相关链接：**

漏洞解释页面：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200005

微软补丁相关页面：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796