### 奇安信CVE-2020-0796快速扫描检测工具使用手册

“奇安信CVE-2020-0796快速扫描检测工具” Microsoft SMBv3远程代码执行漏洞CVE-2020-0796”推出的一款远程扫描工具。该工具可以批量快速扫描检测内网是否存在该漏洞。

**一． 工具说明：**

支持IP段批量扫描检测“CVE-2020-0796”漏洞功能。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。

**二、文件信息：**

文件下载地址：<http://dl.qianxin.com/skylar6/CVE-2020-0796scanner.zip>

版本号：1.0.0.1001

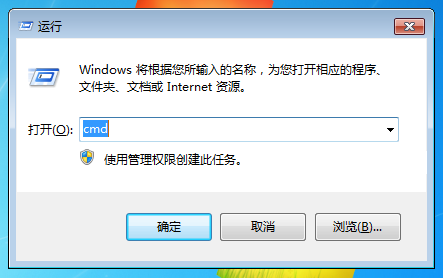
MD5: AA007E57DAAF2D64247FC41EA8A997F4

SHA1: 15B49C05066F5894D254FDD5B3DB126B9D1D2AB9

SHA256: 067B6E17E5F3D9EC070FEF304B57A3F4F7446356231179C573D004AA931262A3

**三、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。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ip或ip范围:192.168.0.2-192.168.0.254

192.168.0.2未发现漏洞(Not vulnerable)

192.168.0.3 有漏洞（Vulnerable）

192.168.0.4 未发现设备（No Client）

以上结果表示：

有漏洞（Vulnerable）-代表检测出漏洞。

未发现漏洞（Not vulnerable）-代表未发现漏洞。

发现设备（No Client）-代表网络故障或不存在该网络设备。

**三、修复“CVE-2020-0796”漏洞**

如果存在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