

奇安信 CVE-2019-0708 漏洞快速扫描检测工具使用手册

“奇安信 CVE-2019-0708 漏洞快速扫描检测工具”是奇安信公司针对“Windows 远程桌面服务的远程代码执行漏洞 CVE-2019-0708”推出的一款远程扫描工具。该工具有两个版本，分别为：快速扫描检测和批量快速扫描检测版本。

一、快速扫描检测工具

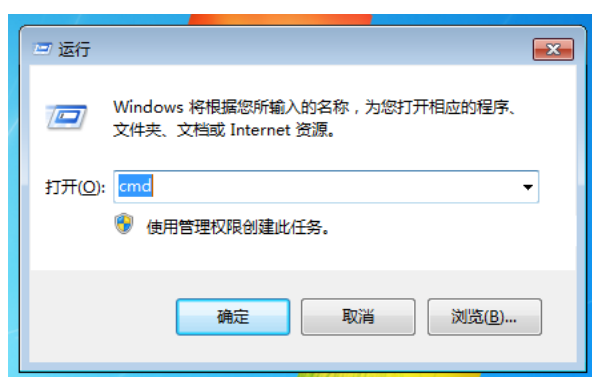
“快速扫描检测工具”具备单 IP 扫描检测“CVE-2019-0708”漏洞功能。适合对单个终端设备进行快速扫描检测。

下载页面：

<https://www.qianxin.com/other/CVE-2019-0708>

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。



- 3、 在命令行工具，输入：快速扫描检测工具的完整路径+IP+端口。回车后可以得到结果。详见如下示例：

```
C:\users\qdy>d:\Downloads\cve-2019-0708-sacn.exe 192.168.0.100 3389
```

```

*****

*      奇安信 CVE-2019-0708 漏洞快速扫描检测工具      *

*      by 奇安信红雨滴 (@RedDrip7) 团队      *

*****

[+] 连接 192.168.0.100:3389 成功...

[+] 警告: SERVER 192.168.0.100 存在漏洞, 系统架构为 x64

```

以上结果表示 192.168.0.100 终端设备系统存在“CVE-2019-0708”漏洞，建议立即修复。

```

C:\users\qdy>d:\Downloads\cve-2019-0708-sacn.exe 192.168.0.101 3389

*****

*      奇安信 CVE-2019-0708 漏洞快速扫描检测工具      *

*      by 奇安信红雨滴 (@RedDrip7) 团队      *

*****

[+] 连接 192.168.0.101:3389 成功...

[*] 恭喜:Server 192.168.0.101 不存在漏洞

```

以上结果表示 192.168.0.101 终端设备系统不存在“CVE-2019-0708”漏洞。

```

C:\users\qdy>d:\Downloads\cve-2019-0708-sacn.exe 192.168.0.102 3389

*****

*      奇安信 CVE-2019-0708 漏洞快速扫描检测工具      *

*      by 奇安信红雨滴 (@RedDrip7) 团队      *

*****

[+] 连接 192.168.0.102:3389 成功...

[*] 恭喜: 192.168.0.102 开启了 NLA, 不存在安全问题

```

以上错误表示 192.168.0.102 终端设备 RDP 服务开启了 NLA 身份验证，不存在安全问题。

```
C:\users\qdy>d:\Downloads\sacn.exe 192.168.0.103 3389

*****

*      奇安信 CVE-2019-0708 漏洞快速扫描检测工具      *
*
*      by 奇安信红雨滴(@RedDrip7) 团队      *
*
*****

[-] 连接 Server 10.95.162.252:3389 错误...

[-] 连接错误...
```

以上错误表示 192.168.0.103 终端设备无法连接，建议检查网络是否畅通。

二、批量快速扫描检测工具

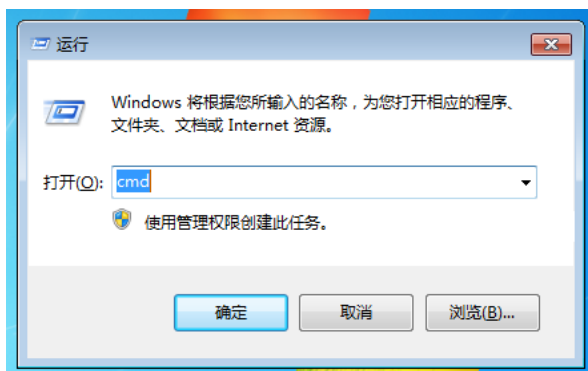
支持 IP 段批量扫描检测“CVE-2019-0708”漏洞功能。适合对局域网全网段扫描，以快速找到局域网内存在该漏洞的全部终端设备。

获取方式：

通过邮箱发送邮件联系：kefu@qianxin.com 索取。

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。



- 3、 在命令行工具，输入：快速扫描检测工具的完整路径+IP1-IP2+端口。回车后可以得到结果，详见如下示例：

```
C:\users\qdy>d:\Downloads\cve-2019-0708-sacn.exe 192.168.0.100-192.168.0.103 3389

*****

*      奇安信 CVE-2019-0708 漏洞快速扫描检测工具      *

*      by 奇安信红雨滴 (@RedDrip7) 团队      *

*****

[+] 连接 192.168.0.100:3389 成功...

[+] 警告: SERVER 192.168.0.100 存在漏洞, 系统架构为 x64

[+] 连接 192.168.0.101:3389 成功...

[*] 恭喜:Server 192.168.0.101 不存在漏洞

[+] 连接 192.168.0.102:3389 成功...

[*] 恭喜: 192.168.0.102 开启了 NLA, 不存在安全问题

[-] 连接 Server 192.168.0.103:3389 错误...
```

以上结果表示 192.168.0.100 终端设备系统存在“CVE-2019-0708”漏洞，建议立即修复。

192.168.0.101 终端设备系统不存在“CVE-2019-0708”漏洞。

192.168.0.102 终端设备 RDP 服务开启了 NLA 身份验证，不存在安全问题。

192.168.0.103 终端设备无法连接，建议检查网络是否畅通。

三、修复“CVE-2019-0708”漏洞

如果检测到相关漏洞的终端设备，建议立即将该设备中的 RDP 服务关闭，同时对该设备进行打补丁相关操作。待打完相关补丁后方可重新开启 RDP 服务。

如需要专修工具或了解如何打该“CVE-2019-0708”漏洞相关补丁，可以到奇安信
官网相关网址查看并下载相关工具：<https://www.qianxin.com/other/CVE-2019-0708>。

特别鸣谢：奇安信红雨滴(@RedDrip7)团队 提供强大技术支持！