

# 微软远程桌面服务远程代码执行漏洞（CVE-2019-0708）预 警通告

## 文档信息

编号	QiAnXinTI-SV-2019-0006
关键字	RDP CVE-2019-0708
发布日期	2019年05月15日
更新日期	2019年05月31日
TLP	WHITE
分析团队	奇安信威胁情报中心

## 通告概述

2019年05月15日，微软公布了5月的补丁更新列表，在其中存在一个被标记为严重的RDP（远程桌面服务）远程代码执行漏洞，攻击者可以利用此漏洞远程无需用户验证通过发送构造特殊的恶意数据在目标系统上执行恶意代码，从而获取机器的完全控制。此漏洞主要影响的设备为Windows 7、Window Server 2008以及微软已不再支持的Windows 2003、Window XP操作系统，涉及系统在国内依然有大量的使用，所以此漏洞的影响面巨大，初步的互联网评估国内受影响RDP服务器达到30万量级IP。由于漏洞利用无需用户交互的特性结合巨大的影响面，意味着该漏洞极有可能被蠕虫所利用，如果漏洞利用稳定有可能导致类似WannaCry蠕虫泛滥的情况发生。

奇安信威胁情报中心红雨滴团队第一时间跟进该漏洞并保持关注，目前已经确认利用此漏洞可以至少非常稳定地触发受影响系统蓝屏崩溃从而导致拒绝服务，到5月31日已有公开渠道发布可以导致系统蓝屏崩溃的POC代码出现，有企图的攻击者可以利用此POC工具对大量存在漏洞的系统执行远程拒绝服务攻击，至此已经构成了非常现实的威胁。

相关厂商微软针对此漏洞已经发布了安全补丁（包括那些已经不再提供技术支持的老旧操作系统），强烈建议用户立即安装相应的补丁或其他缓解措施以避免受到相关的威胁。

## 漏洞概要

漏洞名称	Microsoft Windows Remote Desktop Services 远程代码执行漏洞				
威胁类型	远程代码执行	威胁等级	严重	漏洞ID	CVE-2019-0708
利用场景	未经身份验证的攻击者可以通过发送特殊构造的数据包触发漏洞，可能导致远程无需用户验证控制系统。				
受影响系统及应用版本					

Windows 7 for 32-bit Systems Service Pack 1  
Windows 7 for x64-based Systems Service Pack 1  
Windows Server 2008 for 32-bit Systems Service Pack 2  
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)  
Windows Server 2008 for Itanium-Based Systems Service Pack 2  
Windows Server 2008 for x64-based Systems Service Pack 2  
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)  
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1  
Windows Server 2008 R2 for x64-based Systems Service Pack 1  
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

## 漏洞描述

漏洞存在 Windows 的 Remote Desktop Services（远程桌面服务）中，技术细节已知但在此不再详述，对于漏洞的利用无需用户验证，通过构造恶意请求即可触发导致任意指令执行，系统受到非授权控制。

## 影响面评估

此漏洞影响 Windows 7、Window Server 2008 以及微软已不再支持的 Windows 2003、Window XP 操作系统，目前通过技术评估，还存在大量未安装补丁的 RDP 服务在线，影响面巨大。而且，已有公开渠道发布直接可导致存在漏洞的 RDP 服务所在系统蓝屏崩溃的 POC，形成非常明确急迫的现实威胁，需要引起高度重视。

根据奇安信全球鹰系统的监测，国内存在漏洞并通过互联网可被远程攻击的 IP 数在 **30 万** 级别，每天以差不多 5000 的量缓慢下降，漏洞的修复状况不容乐观。

除此之外，从全球范围来看，目前大约有 **95 万台** 在外网开放远程桌面服务的设备并存在此漏洞的设备，并且还有数不胜数的存在该漏洞的内网设备没有统计，因此如果有效的漏洞利用工具一旦披露，后果不堪设想。

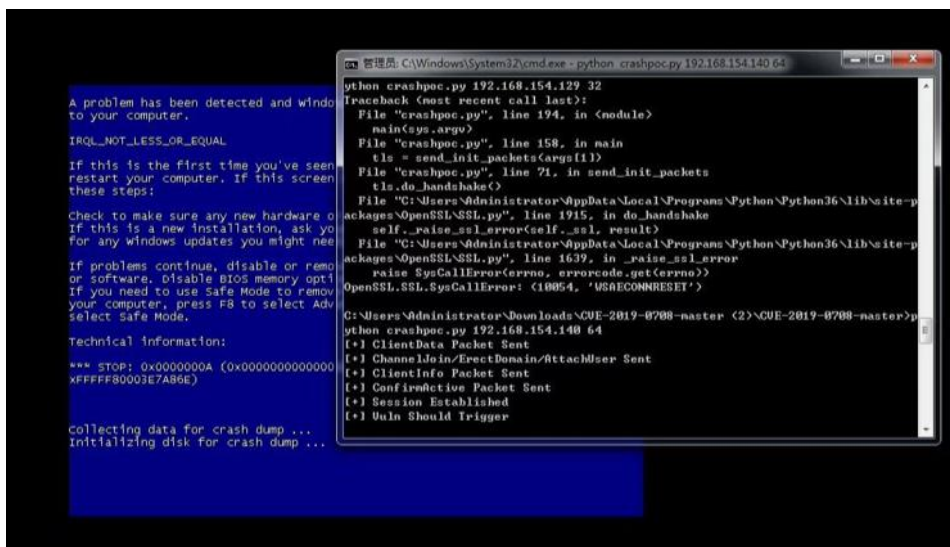
## 漏洞相关事件时间线

奇安信威胁情报中心总结了从微软进行漏洞通告到公开渠道出现能导致蓝屏的 POC 代码的时间线如下：

### 微软远程桌面服务远程代码执行漏洞 ( CVE-2019-0708 ) BlueKeep相关时间线



可以导致蓝屏的 POC 代码已经在公开渠道发布，奇安信威胁情报中心已经确认了 POC 代码的可用性：



结合目前已经有黑客进行大规模扫描存在漏洞设备并进行收集的情况，很有可能导致现实中存在漏洞的主机被批量进行漏洞攻击而导致大规模拒绝服务，请务必对资产进行检查，并升级设备。

## 处置建议

## 修复方法

1. 目前软件厂商微软已经发布了漏洞相应的补丁，奇安信威胁情报中心建议进行相关升级  
<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708#ID0EWIAC>  
Windows XP 及 Windows 2003 可以在以下链接下载补丁：  
<https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708>
2. 奇安信公司推出了针对性的“CVE-2019-0708”漏洞检测修复工具 1.0.0.1004 版：  
<https://www.qianxin.com/other/CVE-2019-0708>  
奇安信公司的其他安全产品：天堤防火墙、天眼高级威胁检测系统、SOC 及态势感知系统都已经支持对于此漏洞利用的检测和防护。
3. 如暂时无法更新补丁，可以通过在系统上启用网络及身份认证（NLA）以暂时规避该漏洞影响。
4. 在企业外围防火墙阻断 TCP 端口 3389 的连接，或对相关服务器做访问来源过滤，只允许可信 IP 连接。
5. 如无明确的需求，可禁用远程桌面服务。

## 参考资料

<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708#ID0EWIAC>  
<https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/>  
<https://www.qianxin.com/other/CVE-2019-0708>

