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 09 月 07 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，到 2019 年 9 月 7 日，奇安信全球鹰系统评估互联网上国内可被直接攻击的受影响 RDP 服务器还有 10 万量级。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。

奇安信息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 2019 年 9 月 7 日，已有可导致远程代码执行的 Metasploit 模块公开发布，随着相关技术的扩散，已经构成了蠕虫级的现实安全威胁。

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，至 2019 年 9 月 7 日已有公开渠道发布可导致远程命令执行的漏洞利用 Metasploit 模块发布，形成非常明确急迫的蠕虫级现实威胁，需要引起高度重视。

根据奇安信全球鹰系统的监测，随着漏洞被逐步地修补，国内存在漏洞并通过互联网可被远程攻击的 IP 数在 10 万量级，漏洞的修复状况不容乐观。

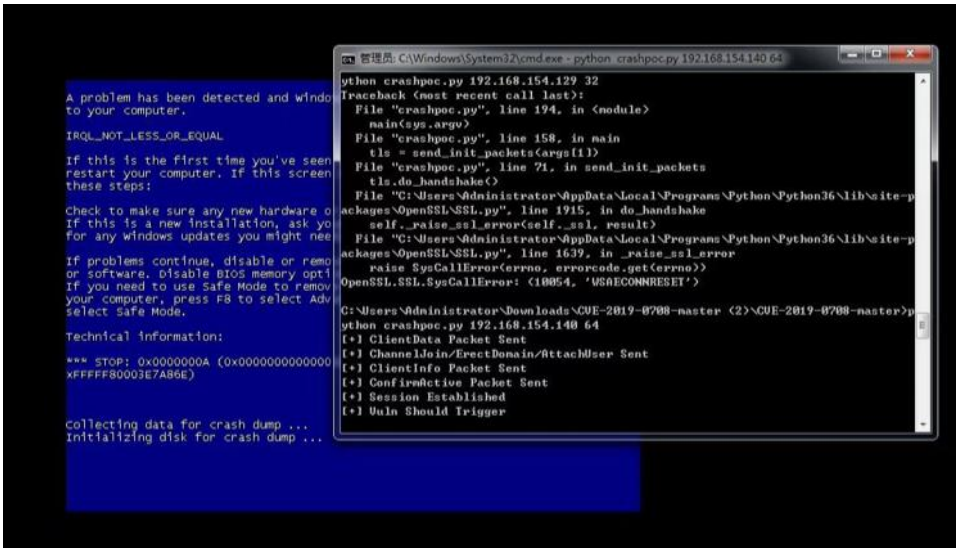
漏洞相关事件时间线

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远程代码执行的 POC 代码的时间线如下：

1. 2019 年 5 月 14 日
   微软发布远程桌面服务代码执行漏洞 CVE-2019-0708 的安全通告及相应补丁，并特别针

对此漏洞发布了专门的说明，提示这是一个可能导致蠕虫泛滥的严重漏洞。

2. 2019 年 5 月 15 日
   奇安信威胁情报中心发布漏洞预警及处置方案，随后奇安信安全产品线发布漏洞检测修复工具。
3. 2019 年 5 月 22 日
   奇安信红雨滴团队发布非破坏性漏洞扫描工具并更新至奇安信漏洞检测修复工具中。
4. 2019 年 5 月 23 日
   互联网公开渠道出现具有非破坏性漏洞扫描功能的 POC 程序。
5. 2019 年 5 月 25 日
   黑客开始大规模扫描存在漏洞的设备。
6. 2019 年 5 月 30 日
   微软再次发布对于 CVE-2019-0708 漏洞做修补的提醒，基于漏洞的严重性强烈建议用户尽快升级修复。
7. 2019 年 5 月 31 日
   互联网公开渠道出现能导致蓝屏的 POC 代码，奇安信威胁情报中心红雨滴团队已经确认了 POC 代码的可用性，漏洞相关的现实威胁进一步升级。



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，奇安信威胁情报中心提醒务必对资产进行检查，并修补设备的漏洞。

8. 2019 年 7 月 31 日
   商业漏洞利用套件 Canvas 加入了 CVE-2019-0708 的漏洞利用模块。
9. 2019 年 9 月 7 日
   已有公开渠道的 Metasploit CVE-2019-0708 漏洞利用模块发布，攻击模块的可用性已经得到验证，当前已构成现实的蠕虫威胁。

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。

临时解决方案

1. 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。
2. 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。
3. 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
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708#ID0EWIAC
https://github.com/busterb/metasploit-framework/blob/bluekeep/modules/exploits/windows/rdp/cve_2019_0708_bluekeep_rce.rb