【漏洞通告】Windows RDP服务远程代码执行漏洞通告(CVE-2019-0708)

原创：QT Lab 青藤实验室

1. 漏洞概述

远程桌面协议（RDP, Remote Desktop Protocol）是一个多通道（multi-channel）的协议，让用户（客户端或称“本地电脑”）连上提供微软终端机服务的电脑（服务器端或称“远程电脑”）是大部分的Windows都有客户端所需软件，RDP服务默认监听本机3389端口。

根据MSRC公告显示，本漏洞为RDP服务远程代码执行漏洞，未经认证的恶意攻击者通过向目标主机RDP服务所在端口发送精心构造的请求，即可在目标主机执行任意代码。该漏洞利用门槛低，危害大且攻击者可通过该漏洞横向蠕虫传播，感染大量主机，危害效果可堪比2017年WannaCry等具备勒索能力的恶意程序。

目前官方暂未公开漏洞细节，建议受影响用户尽快安装补丁进行更新，修复此漏洞。

2. 影响版本

Windows 7
Windows Server 2008
Windows Server 2008 R2
Windows XP
Windows Server 2003

3. 不受影响版本

Windows 8
Windows 10

4. 修复方案

微软官方已经发布更新补丁（包括官方停止维护版本），请用户及时进行补丁更新。

用户可通过微软自动更新功能、WSUS服务或下载补丁方式修复该漏洞，下表

为不同操作系统对应补丁链接：

操作系统版本	补丁下载链接
Windows 7 x86	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.1-kb 499175-x86_6f1319c32d5bc4caf2058ae8ff40789ab 10bf41b.msu
Windows 7 x64	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.1-kb 499175-x64_3704acfff45ddf163d8049683d5a3b75 e49b58cb.msu
Windows Embedded Standard 7 for x64	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.1-kb 499175-x64_3704acfff45ddf163d8049683d5a3b75 e49b58cb.msu
Windows Embedded Standard 7 for x86	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.1-kb 499175-x86_6f1319c32d5bc4caf2058ae8ff40789ab 10bf41b.msu
Windows Server 2008 x64	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.0-kb 499149-x64_9236b098f7cea864f7638e7d4b77aa8f 81f70fd6.msu
Windows Server 2008 Itanium	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.0-kb 499180-ia64_805e448d48ab8b1401377ab9845f39 1cae836d4.msu
Windows Server 2008 x86	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.0-kb 499149-x86_832cf179b302b861c83f2a92acc5e2a1 52405377.msu
Windows Server 2008 R2 Itanium	http://download.windowsupdate.com/c/msdownlo ad/update/software/secu/2019/05/windows6.1-kb 499175-ia64_fabc8e54caa0d31a5abe8a0b347ab4a 77aa98c36.msu
Windows Server 2	http://download.windowsupdate.com/d/msdownlo ad/update/software/secu/2019/05/windows6.1-kb

008 R2 x64	499175-x64_3704acfff45ddf163d8049683d5a3b75e49b58cb.msu
Windows Server 2003 x86	http://download.windowsupdate.com/d/csa/csa/secu/2019/04/windowsserver2003-kb4500331-x86-custom-chs_4892823f525d9d532ed3ae36fc4403382b46a72.exe
Windows Server 2003 x64	http://download.windowsupdate.com/d/csa/csa/secu/2019/04/windowsserver2003-kb4500331-x64-custom-chs_f2f949a9a764ff93ea13095a0aca1fc5071320d3c.exe
Windows XP SP3	http://download.windowsupdate.com/c/csa/csa/secu/2019/04/windowsxp-kb4500331-x86-custom-cs_718543e86e06b08b568826ac13c05f967392238cexe
Windows XP SP2 for x64	http://download.windowsupdate.com/d/csa/csa/secu/2019/04/windowsserver2003-kb4500331-x64-custom-enu_e2fd240c402134839cfa22227b11a5ec80ddafcf.exe
Windows XP SP3 for XPe	http://download.windowsupdate.com/d/csa/csa/secu/2019/04/windowsxp-kb4500331-x86-embedded-custom-chs_96da48aaa9d9bcfe6cd820f239db2f96500bfae.exe
WES09 and POSReady 2009	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/04/windowsxp-kb4500331-x86-embedded-chs_e3fceca22313ca5cdda811f49a606a6632b51c1c.exe

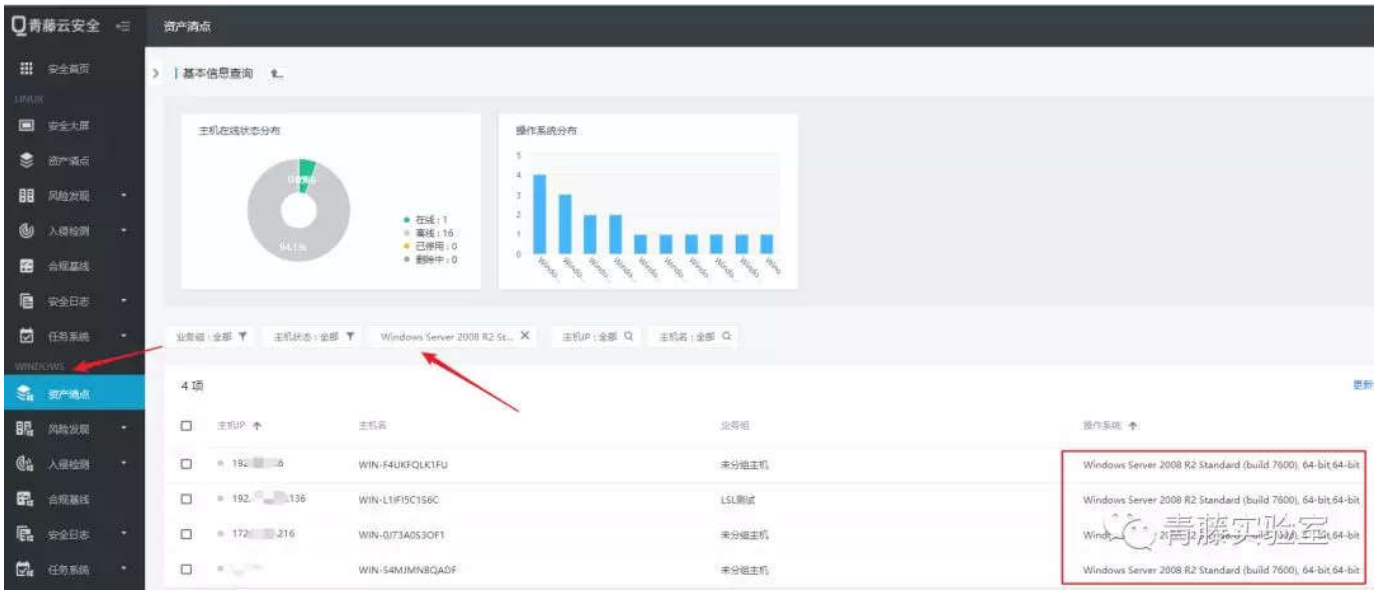
5. 临时修复方案

若用户暂不方便安装补丁更新，可采取下列临时防护措施，对此漏洞进行防护。

1. 若用户不需要用到远程桌面服务，建议禁用该服务。
2. 在主机防火墙中对远程桌面TCP 端口（默认为 3389）进行阻断。
3. 启用网络级认证（NLA），此方案适用于Windows 7, Windows Server 2008, Windows Server 2008 R2。

6. 检查方法

对于启用青藤万相平台Windows模块的用户，登录青藤主机平台，选择Windows模块下的资产清点——主机管理——主机基本信息，通过筛选操作系统版本确定影响范围。



参考链接

https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-wo
by-updating-remote-desktop-services-cve-2019-0708/?
from=groupmessage&isappinstalled=0
https://portal.msrc.microsoft.com/en-US/security-
guidance/advisory/CVE-2019-0708