江西省网络与信息安全情况通报

江西省网络与信息安全信息通报中心　　2019年5月16日

关于Windows远程桌面服务远程代码执行漏洞的预警通报

2019年5月15日，微软发布安全补丁修复了CVE编号为CVE-2019-0708的Windows远程桌面服务（RDP）远程代码执行漏洞，Windows 远程桌面服务（RDP）主要用于管理人员对 Windows 服务器进行远程管理，使用量极大。该漏洞在不需身份认证的情况下即可远程触发，成功利用此漏洞的攻击者可在目标系统上执行任意代码，可安装应用程序，查看、更改或删除数据，创建完全访问权限的新账户等，危害与影响面极大。我中心工作发现我省共有 5985 台设备对外开放 3389 端口，可能受到漏洞影响。请各单位各部门高度重视，立即修复该安全漏洞，具体措施如下:

1、根据微软官方推出的安全更新，参考以下官方安全通告下载并安装最新补丁:

https://support.microsoft.com/zh-cn/help/4500705/customer-guidance-for-cve-2019-0708

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

2、根据以下表格查找对应的系统版本下载最新补丁:

操作系统版本	补丁下载链接
Windows 7 x86	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.1-kb4499175-x86_6f1319c32d5bc4caf2058ae8ff40789ab10bf41b.msu
Windows 7 x64	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.1-kb4499175-x64_3704acfff45ddf163d8049683d5a3b75e49b58cb.msu
Windows Embedded Standard 7 for x64	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.1-kb4499175-x64_3704acfff45ddf163d8049683d5a3b75e49b58cb.msu
Windows Embedded Standard 7 for x86	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.1-kb4499175-x86_6f1319c32d5bc4caf2058ae8ff40789ab10bf41b.msu
Windows Server 2008 x64	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/window

	s6.0-kb4499149-x64_9236b098f7cea864f7638e7d4b77aa8f81f70fd6.msu
Windows Server 2008 Itanium	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.0-kb4499180-ia64_805e448d48ab8b1401377ab9845f39e1cae836d4.msu
Windows Server 2008 x86	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.0-kb4499149-x86_832cf179b302b861c83f2a92acc5e2a152405377.msu
Windows Server 2008 R2 Itanium	http://download.windowsupdate.com/c/msdownload/update/software/secu/2019/05/windows6.1-kb4499175-ia64_fabc8e54caa0d31a5abe8a0b347ab4a77aa98c36.msu
Windows Server 2008 R2 x64	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/05/windows6.1-kb4499175-x64_3704acfff45ddf163d8049683d5a3b75e49b58cb.msu
Windows Server 2003 x86	http://download.windowsupdate.com/d/csa/csa/secu/2019/04/windowsserver2003-kb4500331-x86-custom-chs_4892823f525d9d532ed3ae3

	6fc440338d2b46a72.exe
Windows Server 2003 x64	http://download.windowsupdate.com/d/csa/csa/secu/2019/04/windowsserver2003-kb4500331-x64-custom-chs_f2f949a9a764ff93ea13095a0aca1fc507320d3c.exe
Windows XP SP3	http://download.windowsupdate.com/c/csa/csa/secu/2019/04/windowsxp-kb4500331-x86-custom-chs_718543e86e06b08b568826ac13c05f967392238c.exe
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_96da48aaa9d9bcfe6cd820f239db2fe96500bfae.exe
WES09 and POSReady 2009	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/04/windowsxp-kb4500331-x86-embedded-chs_e3fceca223

	13ca5cdda811f49a606a6632b51c1c.exe

3、缓解措施:

如无法更新补丁，可以通过在系统上启动 NLA（网络级别身份认证）暂时规避该漏洞风险；在企业边界防火墙阻断 TCP 协议 inbound 3389 的连接，或只允许可信 IP 进行连接；如无明确要求，可选择禁用 3389（远程桌面服务）。

附：1、漏洞影响范围

2、产品解决方案

联系人：葛建文，联系电话：0791-87288378。

省网络与信息安全信息通报中心

2019 年 5 月 16 日

附件 1、漏洞影响范围

- 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)
- Windows XP SP3 x86
- Windows XP Professional x64 Edition SP2
- Windows XP Embedded SP3 x86
- Windows Server 2003 SP2 x86

- Windows Server 2003 x64 Edition SP2

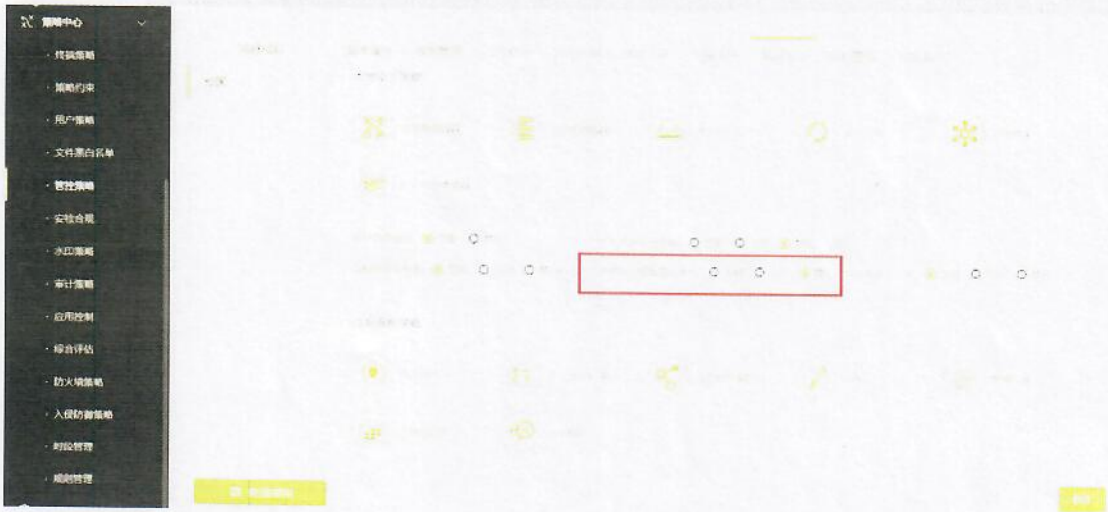
附件 2、产品解决方案

1、使用天擎策略禁止远程桌面到终端。

a) 登录天擎控制台，进入策略中心——管控策略，创建新模板（或修改原有模板）

b) 启用“桌面加固”，将“计算机远程桌面到本机”设置为“禁用”。

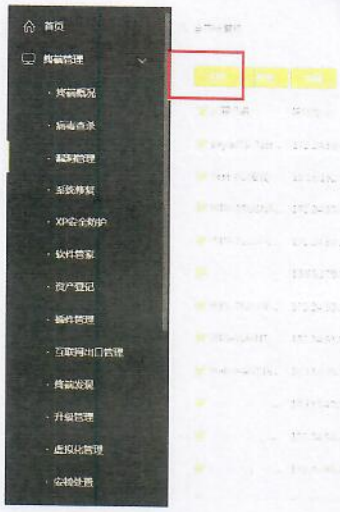
c) 分发该策略到全网计算机。



2、更新奇安信集团 2019.05.15.1 版本及之后的补丁库。

a) 在策略中心修改策略为“安装补丁后自动重启”，系统补丁安装后必须要重启，否则并没有修复漏洞，仍然会被利用攻击。（6.6 版本支持，其他版本的用户在单点维护中单点的下发重启任务，或者通过别的方法要求终端用户配合重启）

b) 在天擎控制台——终端管理——漏洞管理——按终端显示，下发全网扫描任务，让所有的终端扫描补丁情况。



c) 在天擎控制台——终端管理——漏洞管理——按漏洞显示，找到需要紧急的漏洞对应的补丁，手动按分组分多个批次下发修复任务。