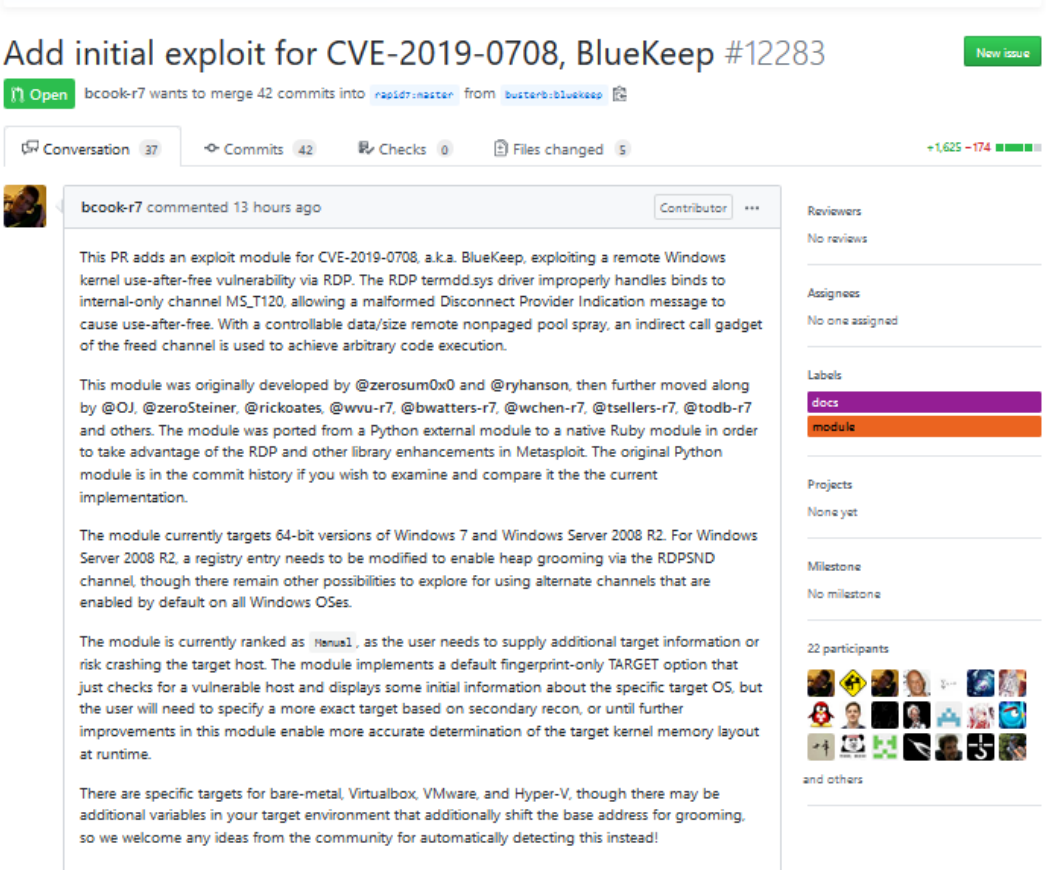
Windows 远程桌面服务远程代码执行漏洞（CVE-2019-0708）EXP 披露预警通告

■ 预警编号	NS-2019-0017-2	■ 发布日期	2019-09-07
■ 危害等级	高，此漏洞影响远程桌面服务，可被用于实现蠕虫攻击，请尽快安装更新补丁，修复此漏洞。EXP 已公布。		
■ TAG	Windows、远程桌面服务、Remote Desktop Service、远程代码执行、CVE-2019-0708		

一. EXP 披露

北京时间 9 月 7 日凌晨，有开发者在 GitHub 上披露了 Windows 远程桌面服务远程代码执行漏洞 (CVE-2019-0708) 的 Metasploit 利用模块，本次的 CVE-2019-0708（BlueKeep）的初始公共漏洞模块可导致旧版本的 Windows（Windows 7 SP1 x64 与 Windows 2008 R2 x64）无交互远程代码执行。随着工具的扩散，该漏洞有可能导致类似 WannaCry 泛滥的情况发生，已经构成了蠕虫级的现实安全威胁。



经测试该 EXP 已经可以利用成功。Metasploit 的 BlueKeep 利用模块默认仅识别目标操作系统版本以及目标是否可能易受攻击。该 EXP 目前无法实现准确的自动化攻击；它要求用户在进一步利用之前手动对目标详细信息进行配置。如果模块在利用时未能正确的配置参数，则可能导致目标主机蓝屏崩溃，目前已有黑客进行大规模扫描存在漏洞设备的情况，可能导致现实中存在漏洞的主机被批量进行漏洞攻击。**在此强烈建议用户务必对资产进行检查，对受影响设备立即安装相应的补丁或采取其他缓解措施以避免受到相关的威胁。**

EXP 参考链接：

https://github.com/rapid7/metasploit-framework/pull/12283?from=timeline&isappinstalled=0

https://github.com/rapid7/metasploit-framework/pull/12283/files

二. 漏洞概述

北京时间 5 月 15 日，微软官方发布了 5 月安全更新补丁，此次更新共修复了 82 个漏洞，其中 Windows 操作系统远程桌面服务漏洞（CVE-2019-0708）威胁程度较高，攻击者可通过 RDP 协议向目标发送恶意构造请求，实现远程代码执行，甚至可利用此漏洞实现蠕虫式攻击。

鉴于此漏洞的威胁程度较高，针对已经停止维护的 Windows 版本微软也发布了安全补丁。目前针对此漏洞的 EXP 已公布，建议受影响用户尽快安装补丁进行更新，修复此漏洞。

官方参考链接：

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

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

三. 影响范围

受影响版本

- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack1
- Windows Server 2008 for 32-bit SystemsService Pack 2
- Windows Server 2008 for 32-bit SystemsService Pack 2 (Server Core installation)
- Windows Server 2008 for Itanium-Based SystemsService Pack 2
- Windows Server 2008 for x64-based SystemsService Pack 2
- Windows Server 2008 for x64-based SystemsService Pack 2 (Server Core installation)
- Windows Server 2008 R2 for Itanium-BasedSystems Service Pack 1
- Windows Server 2008 R2 for x64-based SystemsService Pack 1
- Windows Server 2008 R2 for x64-based SystemsService Pack 1 (Server Core installation)
- Windows Server 2003 SP2 x86（已停止维护）
- Windows Server 2003 x64 Edition SP2（已停止维护）

- Windows XP SP3 x86（已停止维护）
- Windows XP Professional x64 Edition SP2（已停止维护）
- Windows XP Embedded SP3 x86（已停止维护）

不受影响版本

- Windows 8
- Windows 10

四. 漏洞检测

4.1 绿盟云线上检测

绿盟云提供在线的检测入口，企业用户可进入页面检测自有资产是否受此漏洞影响。

- 手机端访问地址：
  https://cloud.nsfocus.com/megi/holes/hole_WindowsRDP_2019_5_15.html
- PC 端访问地址：
  https://cloud.nsfocus.com/#/secwarning/secwarning_news

4.2 产品检测

绿盟远程安全评估系统（RSAS）已经针对该漏洞提供了原理扫描规则支持，规则升级包详情见下表：

	升级包版本号	升级包下载链接
RSAS V6 系统插件包	V6.0R02F01.1411	http://update.nsfocus.com/update/downloads/id/28802
RSAS V5 系统插件包	051840	http://update.nsfocus.com/update/downloads/id/28822

关于 RSAS 的配置指导，请参考如下链接：

https://mp.weixin.qq.com/s/aLAWXs5DgRhNHf4WHHhQyg

五. 漏洞防护

5.1 产品防护

针对此漏洞，绿盟科技防护产品已发布规则升级包，可形成针对此漏洞的防护能力。强烈建议相关用户升级至最新规则。安全防护产品规则版本号如下：

安全防护产品	规则版本号	升级包下载链接	规则编号
IPS	5.6.10.20340	http://update.nsfocus.com/update/downloads/id/28804	【24489】
	5.6.9.20340	http://update.nsfocus.com/update/downloads/id/28803	
	5.6.8.778	http://update.nsfocus.com/update/downloads/id/28794	
NF	6.0.1.778	http://update.nsfocus.com/update/downloads/id/28828	

产品规则升级的操作步骤详见如下链接：

IPS：https://mp.weixin.qq.com/s/JsRktENQNj1TdZSU62N0Ww

NF：https://mp.weixin.qq.com/s/bggqcm9VqHiPnfV1XoNuDQ

5.2 官方补丁

微软官方已经发布更新补丁（包括官方停止维护版本），请受影响用户尽快进行补丁更新。获得并安装补丁的方式有三种：内网 WSUS 服务、微软官网 Microsoft Update 服务、离线安装补丁。

注：如果需要立即启动 Windows Update 更新，可以在命令提示符下键入 wuauclt.exe /detectnow。

方式一： 内网 WSUS 服务

适用对象：已加入搭建有 WSUS 服务器内网活动目录域的计算机，或手工设置了访问内网 WSUS 服务。

系统会定时自动下载所需的安全补丁并提示安装，请按提示进行安装和重启系统。

如果希望尽快安装补丁，请重新启动一次计算机即可。

方式二： 微软官网 Microsoft Update 服务

适用对象：所有可以联网，不能使用内网 WSUS 服务的计算机，包括未启用内网 WSUS 服务的计算机、启用了内网 WSUS 服务但未与内网连接的计算机。

未启用内网 WSUS 服务的计算机，请确保 Windows 自动更新启用，按照提示安装补丁并重启计算机。

启用内网 WSUS 服务的计算机但没有与内网连接的计算机，请点击开始菜单-所有程序-Windows Update，点击“在线检查来自 Windows Update 的更新”，按提示进行操作。

方式三： 离线安装补丁

下载对应的补丁安装包，双击运行即可进行修复，下载链接可参考本文“附录 A 官方补丁下载链接”。

5.3 临时解决建议

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、启用网络级别身份认证（NLA），此方案适用于 Windows 7, Windows Server 2008, and Windows Server 2008 R2。

附录A 官方补丁下载链接

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/windows6.0-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_4892823f525d9d532ed3ae36fc440338d2b46a72.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_e3fceca22313ca5cdda811f49a606a6632b51c1c.exe

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、

医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

绿盟科技安全预警微信二维码

绿盟科技官方微信二维码