

在Microsoft的May Patch Tuesday周报中发布了针对远程桌面协议（RDP）中的漏洞安全公告。在这个补丁报告中，微软为Windows XP和其他几个操作系统提供了修复报告，然而这些操作系统多年里并没有得到非常安全的补丁更新支持。这就是为何微软将此漏洞设定为高危的原因所在。

根据该通报，我们发现此问题非常严重，能够导致远程执行代码并非常容易被攻击者利用，这意味着它可以在未受保护的系统上进行自动传播。该公告使用了网络蠕虫“WannaCry”Advanced Threat Research一直在分析这个最新的bug以帮助预防类似的情况，我们敦促那些未修补和受影响的系统尽快应用CVE-2019-0708补丁。恶意行为者极有可能部署此漏洞，并且在

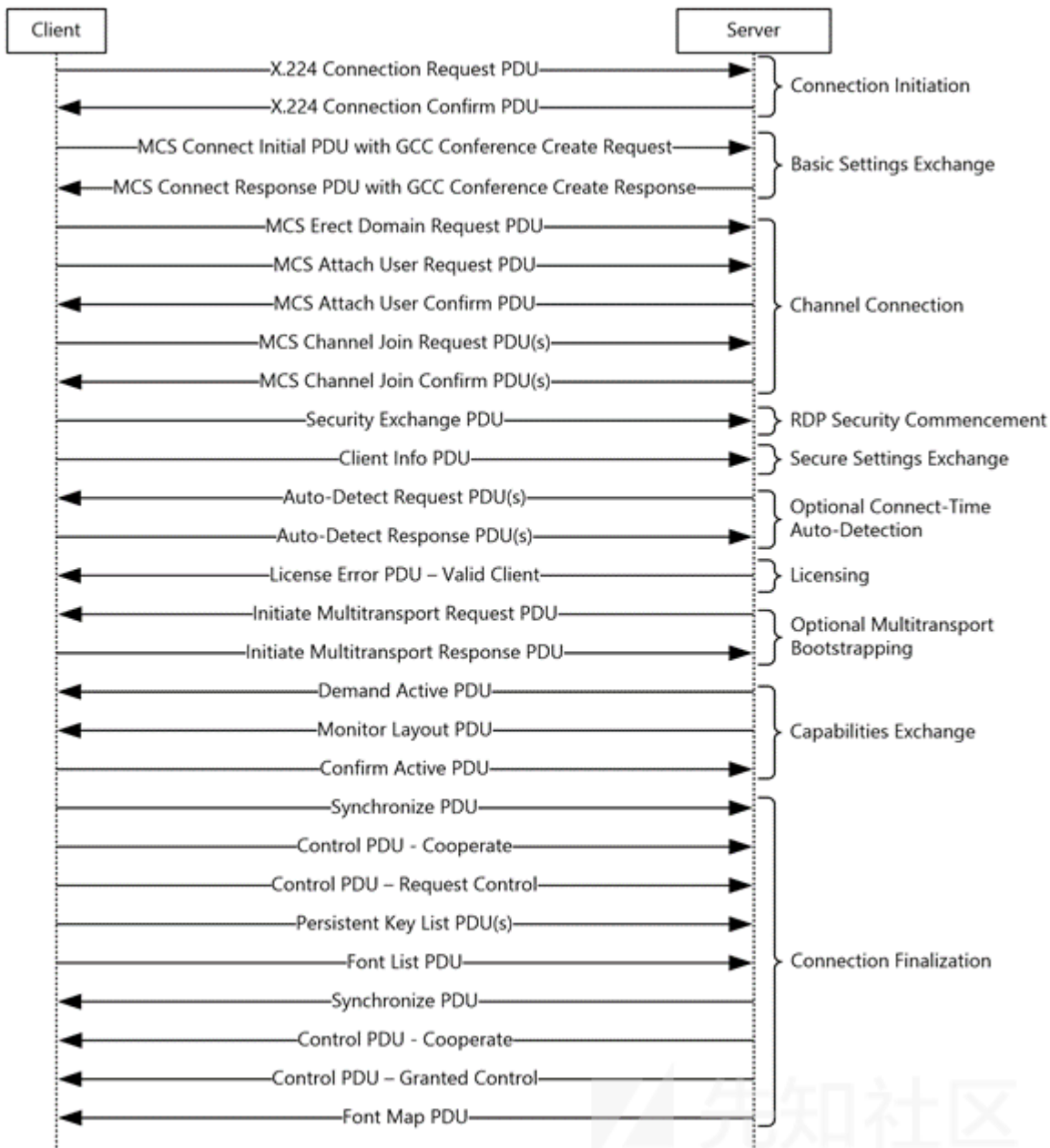
易受攻击的操作系统：

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

蠕虫是主要在网络上复制的病毒。蠕虫通常会在远程计算机上自动执行，而无需用户提供任何额外帮助。如果病毒的主要攻击媒介是通过网络，那么它就被归类为蠕虫病毒。

远程桌面协议（RDP）支持客户端和端点之间的连接，定义虚拟通道之间通信的数据。虚拟通道是双向数据管道，可以扩展RDP。Windows Server 2000使用RDP 5.1定义了32个静态虚拟通道（SVC），但由于定动态虚拟通道（DVC）的通道数量存在限制，这些通道包含在专用SVC中。SVC在会话开始时创建并保持到会话终止，这与需要创建和拆除的DVC不同。

下图为32个SVC绑定信息，CVE-2019-0708补丁修复了RDP驱动程序termdd.sys中的\_IcaBindVirtualChannels和\_IcaRebindVirtualChannels函数。如图所示



该漏洞是由于“MS\_T120”SVC名称在RDP协议的GCC初始化期间被绑定为数字31的参考信道。此通道名称在Microsoft内部使用，并且客户端没有合法用例来请求名为“MS\_T120”的SVC连接。

图2显示了没有MS\_T120信道的GCC初始化序列合法信道请求。

17	3.572395382	192.168.174.1	192.168.174.135	RDP	512 ClientData
<ul style="list-style-type: none"> <li>▶ Frame 17: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface 0</li> <li>▶ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_43:2c:f3 (00:0c:29:43:2c:f3)</li> <li>▶ Internet Protocol Version 4, Src: 192.168.174.1, Dst: 192.168.174.135</li> <li>▶ Transmission Control Protocol, Src Port: 51310, Dst Port: 3389, Seq: 20, Ack: 12, Len: 446</li> <li>▶ TPkt, Version: 3, Length: 446</li> <li>▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol</li> <li>▼ MULTIPOINT-COMMUNICATION-SERVICE T.125 <ul style="list-style-type: none"> <li>▼ ConnectMCSPDU: connect-initial (101) <ul style="list-style-type: none"> <li>▶ connect-initial</li> </ul> </li> </ul> </li> <li>▼ GENERIC-CONFERENCE-CONTROL T.124 <ul style="list-style-type: none"> <li>▼ ConnectData <ul style="list-style-type: none"> <li>▶ t124Identifier: object (0)</li> <li>▼ connectPDU: 000800100001c00044756361813a01c0ea000b0008008007... <ul style="list-style-type: none"> <li>▼ connectGCCPDU: conferenceCreateRequest (0) <ul style="list-style-type: none"> <li>▶ conferenceCreateRequest</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>▼ Remote Desktop Protocol <ul style="list-style-type: none"> <li>▼ ClientData <ul style="list-style-type: none"> <li>▶ clientCoreData</li> <li>▼ clientClusterData <ul style="list-style-type: none"> <li>headerType: clientClusterData (0xc004)</li> <li>headerLength: 12</li> <li>clusterFlags: 0x00000015</li> <li>redirectedSessionId: 0x00000000</li> </ul> </li> <li>▶ clientSecurityData</li> <li>▼ clientNetworkData <ul style="list-style-type: none"> <li>headerType: clientNetworkData (0xc003)</li> <li>headerLength: 56</li> <li>channelCount: 3</li> <li>▼ channelDefArray <ul style="list-style-type: none"> <li>▼ channelDef <ul style="list-style-type: none"> <li>name: rdpdr <ul style="list-style-type: none"> <li>▶ options: 0x80800000</li> </ul> </li> </ul> </li> <li>▼ channelDef <ul style="list-style-type: none"> <li>name: rdpsnd <ul style="list-style-type: none"> <li>▶ options: 0xc0000000</li> </ul> </li> </ul> </li> <li>▼ channelDef <ul style="list-style-type: none"> <li>name: cliprdr <ul style="list-style-type: none"> <li>▶ options: 0xc0a00000</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li></ul>					

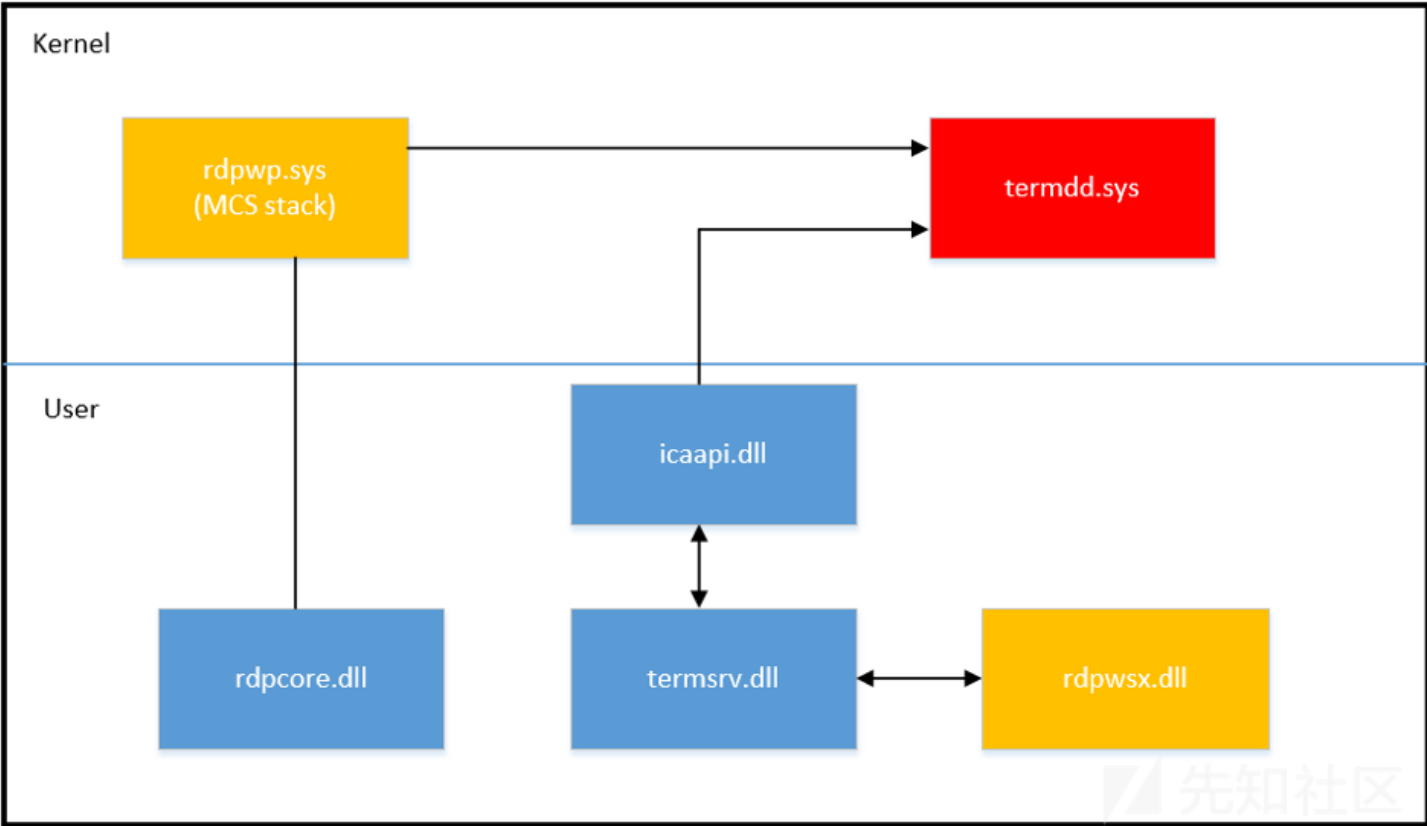


但是，在GCC初始化期间，客户端所提供的服务器中并未列入白名单的频道名称，这意味着攻击者可以在31以外的频道上设置另一个名为“MS\_T120”的SVC。在31以外的频道会导致堆内存损坏和远程代码执行（RCE）。

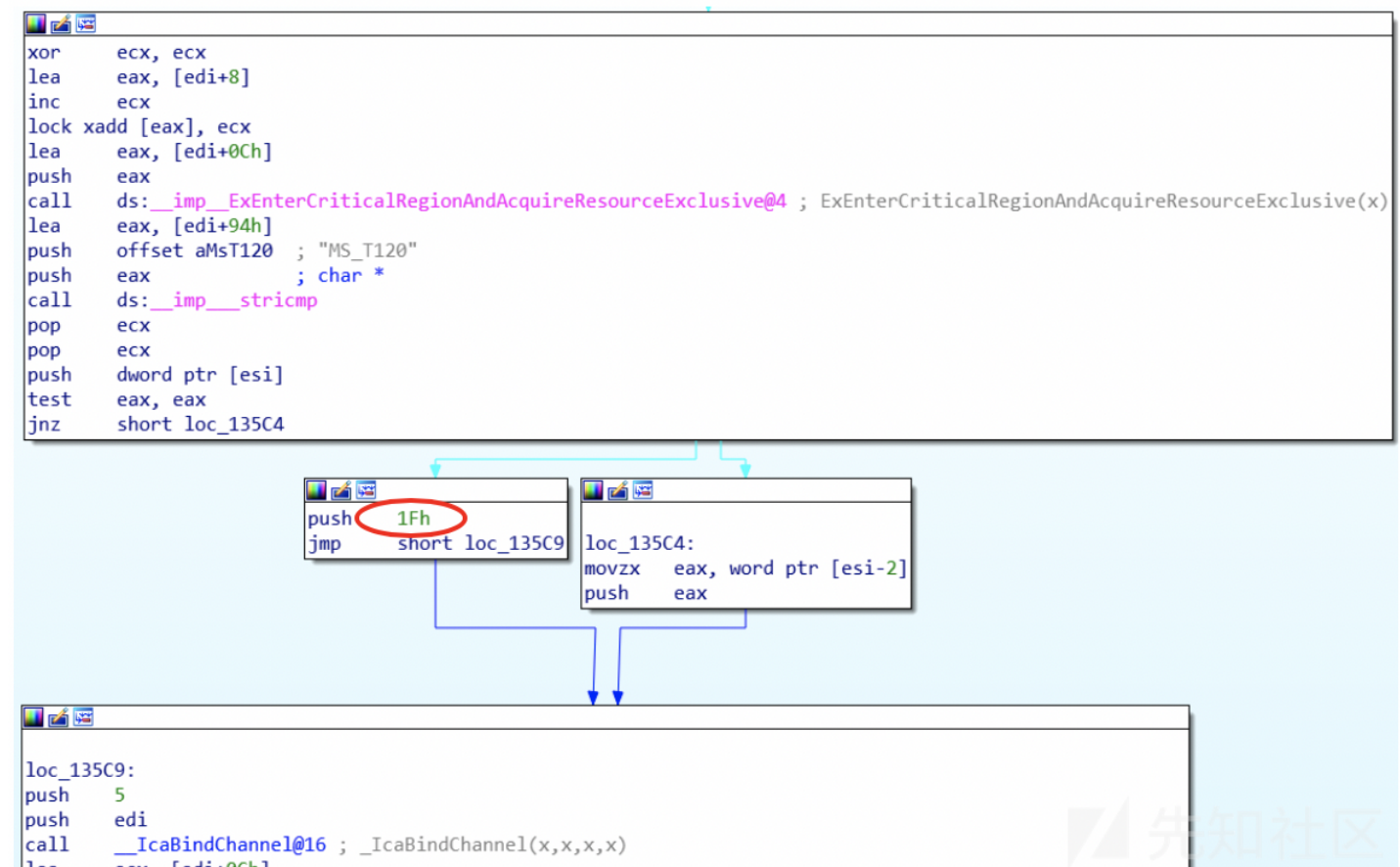
图3显示了GCC会议初始化序列期间的异常信道请求，其信道号为4且名称为“MS\_T120”。

```
12 2.183562573 192.168.174.1 192.168.174.135 RDP 512 ClientData
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
MULTIPOINT-COMMUNICATION-SERVICE T.125
GENERIC-CONFERENCE-CONTROL T.124
  ConnectData
    t124Identifier: object (0)
    object: 0.0.20.124.0.1 (Generic Conference Control)
    connectPDU: 000800100001c00044756361813a01c0ea000b0008008007...
      connectGCCPDU: conferenceCreateRequest (0)
        conferenceCreateRequest
          conferenceName
            0... lockedConference: False
            .0.. listedConference: False
            ..0. conductibleConference: False
          terminationMethod: automatic (0)
          userData: 1 item
Remote Desktop Protocol
  ClientData
    clientCoreData
    clientClusterData
    clientSecurityData
    clientNetworkData
      headerType: clientNetworkData (0xc003)
      headerLength: 56
      channelCount: 4
      channelDefArray
        channelDef
          name: rdpdr
          options: 0x80000000
        channelDef
          name: rdpsnd
          options: 0xc0000000
        channelDef
          name: cliprdr
          options: 0xc0a00000
        channelDef
          name: MS_T120
          options: 0x00000000
          0... .. = optionsInitialized: 0x0
          .0.. .. = encryptRDP: 0x0
          ..0. .. = encryptSC: 0x0
          ...0. .. = encryptCS: 0x0
          ....0. .. = priorityHigh: 0x0
          .....0.. .. = priorityMed: 0x0
          .....0. .. = priorityLow: 0x0
          .....0. .. = compressRDP: 0x0
          .....0. .. = compress: 0x0
          .....0. .. = showProtocol: 0x0
          .....0. .. = remoteControlPersistent: 0x0
```

图4展现了MS\_T120通道管理中涉及的.MS\_D120组件是如何在引用通道rdpwsx.dll和rdpwp.sys中完成堆分配并创建。当在31以外的通道索引的上下文中处理MS\_T120引用通道时，堆损坏发生在termdd.sys中。




现在，如图所示的Microsoft补丁使用通道名称“MS\_T120”添加了对客户端连接请求的检查，并确保它在termdd.sys中的\_IcaBindVirtualChannels和\_IcaRebind



在我们调查了Windows

2003和XP的补丁并了解了如何在补丁之前和之后解析RDP协议后，我们决定创建并测试一个验证脚本（PoC），它将使用该漏洞并远程执行代码在受害者的机器上启动计算

```
C:\BlueKeep>BlueKeep.exe 192.168.0.117  
POC for CVE-2019-0708 (PRIVATE, DONT ASK ABOUT IT!)  
Prepare to send packets without auth to 192.168.0.117 target machine...  
Sending packets!  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
  
Packets sent with success!
```

The logo for XinZhi Community, featuring a stylized 'X' icon followed by the text '先知社区'.

在我们的设置中，RDP在计算机上运行，我们确认测试版本的操作系统上运行了未修补的版本。

通过我们的调查，我们可以确认漏洞利用是否正常，并且可以在没有身份验证的情况下在易受攻击的系统上远程执行代码。如果启用，网络级别身份验证应该有效地阻止此漏洞利用。但是，如果攻击者拥有验证凭证，他们将绕过此步骤。

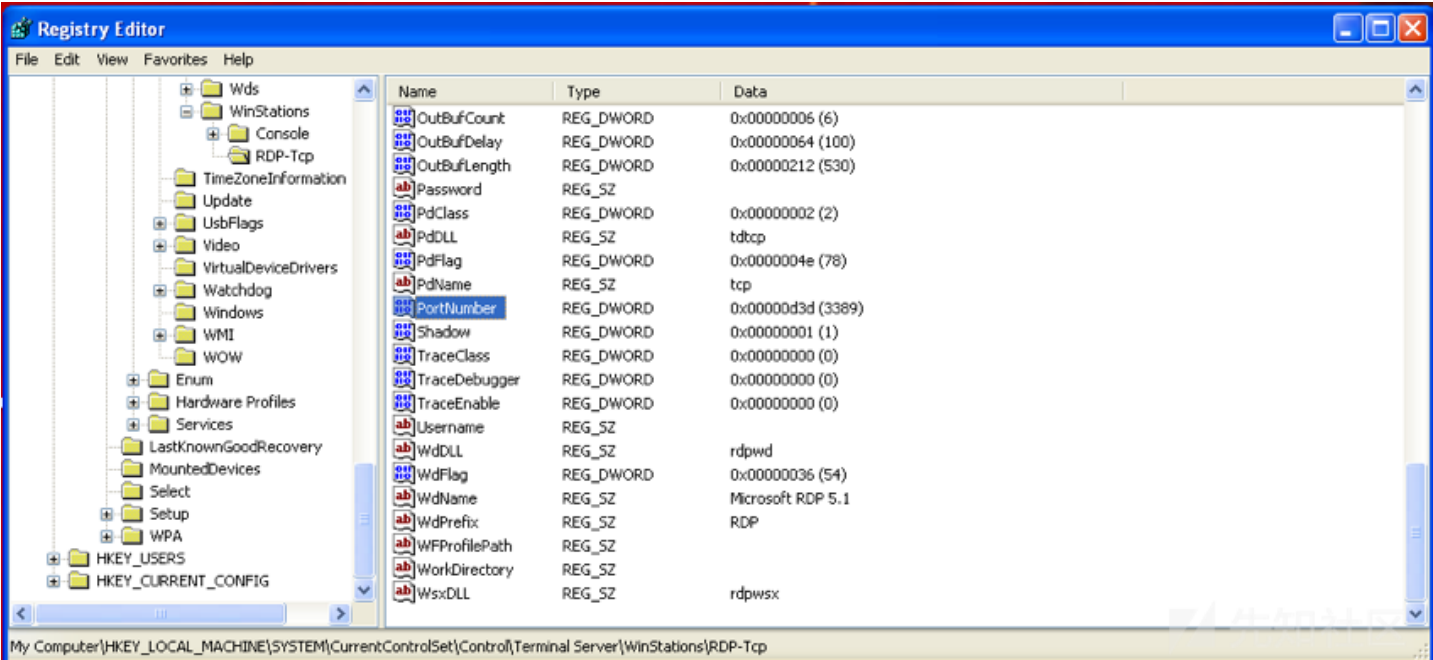
由于补丁可用，我们决定不提供有关漏洞的更深入的详细信息或公开发布POC。

我们可以确认修补后的系统会阻止该漏洞，并强烈建议用户尽快修补。

从网络外部禁用RDP并在内部对其进行限制。禁用RDP时，漏洞利用不成功。

除非有合法使用案例的证据，否则应阻止在RDP协议的GCC会议初始化序列期间在31以外的任何通道上使用“MS\_T120”的客户端请求。

需要注意的是，RDP默认端口可以在注册表字段中进行更改，并且重新启动后将绑定新指定的端口。



公司内部的恶意软件或管理员可以使用管理员权限（或绕过UAC的程序）更改此设置，并在注册表中写入此端口。如果系统未修补，则该漏洞仍可通过唯一端口进行利用。

■■■■■■■■■■[https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-w

点击收藏 | 1 关注 | 1

[上一篇：Hackthebox: kotar...](#) [下一篇：C++逆向学习\(四\) 类](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)