

In the Boxing Ring

2024年2月



Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2024年2月份的 In the Boxing Ring

本月，我们将讨论勒索软件交付协议 (RDP) 等。虽然这是远程桌面协议的文字游戏，但它所带来的安全风险不容忽视。在过去五年中 Network Box 协助处理的每一起勒索软件案件中，RDP 一直是网络渗透和最终勒索软件传播的第一大机制。尽管 RDP 是最严重的问题，但它并不是此类服务中唯一有问题的。在第 2 至 3 页上，我们更详细地讨论了这一点，并提供了一些缓解这些威胁的最佳实践。

其他新闻中，Network Box 董事总经理 Michael Gazeley 参加了题为“共建网络安全屏障 - 开创智慧城市新篇章”的网络安全专题讨论会。此外，作为特别的年终总结，Network Box 将去年的所有重大事件整理在2023年版《Year in Focus》中。在本月的全球安全头条中，出现了 Cisco、TeamViewer、Ivanti 和 Cloudflare 的安全问题。



Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2024

本月摘要:

第2-3页

论勒索软件交付协议 (RDP) 等

这是远程桌面协议的文字游戏。在过去五年中，RDP 一直是网络渗透和最终勒索软件传播的第一大机制。在几乎所有这些情况下，RDP 服务完全不受保护 - 没有源 IP 限制、没有有效的密码策略、没有密码锁定策略，也没有任何限制。然而，RDP 并不是此类服务中唯一有问题的。在我们的专题文章中，我们更详细地讨论了这一点。

第4页

Network Box 亮点:

- Network Box 香港: 数码港网络安全小组讨论
- Network Box Year in Focus 2023
- 全球安全头条:
 - Cisco
 - TeamViewer
 - Ivanti
 - Cloudflare

勒索软件 传送协议 (RDP) 等

想象一下，把笔记本电脑放在家门前的走廊上。虽然它有防盗装置，但任何路过的人都可以使用屏幕、鼠标和键盘进入登录界面“碰碰运气”。他们会反复猜测用户名和密码，直到最终成功登录并访问您的所有文件和应用程序。更糟糕的是，他们还可以利用你的笔记本电脑的网络连接访问你家中的所有其他电脑（绕过前置防火墙的保护）。

听起来很荒谬吧？任何正常人都不会这么做，对吗？今天，通过 Shodan 对 tcp/3389 端口的快速搜索，可以发现超过 460 万台这样的计算机（带鼠标、键盘和屏幕）向公共互联网开放，并绕过了防火墙控制。

向互联网开放 tcp/3389 RDP 最多的国家

#1	China	1.5 million
#2	USA	1.2 million
#3	Germany	214,000
#4	Japan	115,000
#5	Hong Kong	109,000

使用我们的内部 Nidan 工具（类似于 Shodan，但只覆盖 Network Box 管理的网络），显示有几十个 tcp/3389 端口向公共互联网开放。尽管多年来多次发出警告并推荐最佳做法，但情况依然如此。



诚然，我们称 tcp/3389 RDP 为 "勒索软件传输协议"（其正式名称为 "远程桌面协议"）是一种调侃，但我相信你一定明白其中的意思。在过去五年中，Network Box 协助处理的每一个勒索软件案例中，RDP 都是网络渗透和最终勒索软件交付的第一大机制。其他任何方式都无法与之相提并论。而在几乎所有这些案例中，RDP 服务都是完全不受保护的 - 没有源 IP 限制、没有有效的密码策略、没有密码锁定策略，也没有任何限制。

向互联网开放远程管理访问

一般来说，提供管理访问的远程管理访问服务（如 SSH、RDP、VNC 等）不应向互联网开放。向互联网开放此类服务会使网络直接暴露于漏洞或不安全凭证的利用以及暴力攻击之下。由于提权问题，即使是仅限用户（非管理员）访问的服务也不鼓励开放。



尽管 RDP 是最严重的问题，但它并不是此类服务中唯一有问题的。在我们的托管网络中，我们看到超过 1,000 个 tcp/22 (SSH)、700 个 Cisco、300 个 Fortinet、200 个 tcp/23 (TELNET)、150 个 Sonicwall、150 个 tcp/5900 (VNC) 和十几个 Palo Alto 管理接口 直接向公共互联网开放。

在全球范围内，情况更糟：2500 万个 SSH、600 万个 Cisco、67 万个 Fortinet、200 万个 TELNET、86 万个 Sonicwalls 和 60 万个 VNC。可以理解的是，其中许多都在 ISP 提供的路由器设备中 - 鉴于 ISP 将这些设备限制在其 SOC 地址范围的简单性，这是不可原谅的。但许多也特意开放以允许远程访问（特别是新冠疫情后和相关的在家工作安排）。

Network Box 等公司推荐了保护网络安全的最佳做法，其中第一条就是防止 "向互联网开放远程管理访问"。

作为替代方案，建议部署 VPN/SDWAN 服务。这些远程管理服务只能通过安全的 VPN/SDWAN 链接提供给特定的用户账户、VPN 端点或源 IP 地址。



我们过去写过这方面的文章，毫无疑问，今后还会再写。归根结底，安全策略是由我们的客户来维护的；Network Box 只能指出其中的危险，并提出修改建议。尽管如此，如果您的管理服务开放至互联网，尤其是 RDP tcp/3389，那么无论您的网络是否受 Network Box 保护，如果您只需作出一项更改以加强网络保安，那就是将其锁住。

部署和使用 SSL VPN 技术在这些协议之上提供一层身份验证是比较简单的，把这些服务放在这样的 VPN 后面，就等于把笔记本电脑从门廊前移到安全的地方，路人无法轻易篡改它。

Network Box HIGHLIGHTS



Network Box 香港网络安全小组讨论

Network Box 董事总经理 Michael Gazeley 于香港数码港出席一个名为「共建网络安全屏障 - 开创智慧城市新篇章」的网络安全专题讨论会。在讨论中，小组成员分享了加强网络安全的案例和经验，让科技创新的应用有更安全和有利的网络环境，从而推动智慧城市的发展。



全球安全头条:



黑暗阅读

关键的思科统一通信 RCE 错误允许root访问

LINK: <https://bit.ly/42nKsep>



Bleeping Computer

TeamViewer 在新的勒索软件攻击中被滥用来破坏网络

LINK: <https://bit.ly/3weGhpt>



Security Week

延迟后, Ivanti 修补了零日漏洞并确认了新漏洞

LINK: <https://bit.ly/3Ut31vv>



The Hacker News

Cloudflare 漏洞: 国家黑客获取源代码和内部文件

LINK: <https://bit.ly/3SKB5Sx>

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOG
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581
www.network-box.cn

Network Box Year in Focus 2023



作为年终特别总结, Network Box 将过去 12 个月中的所有重要事件编入 2023 年版的《Year in FOCUS》中。

LINK:
<https://bit.ly/3w16TKi>