防御 Windows RDP 攻击

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Defending against Windows RDP attacks		
原文作者	马克·中柏（Mike Jumper）	**原文发布日期**	2021 年 5 月 10 日
作者简介	马克·中柏是 Glyptodon 公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/05/10/windows-rdp-attacks/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	在新的远程工作环境中，RDP 将继续在实现对虚拟和物理企业计算机的远程访问方面发挥关键作用。通过一些相对简单的措施（及时打补丁、将 RDP 部署在安全网关之后，以及采用最低权限原则），企业可以安全地提供远程访问，不必担心会为黑客提供新的漏洞。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

防御 Windows RDP 攻击

马克·中柏

2021 年 5 月 10 日

根据 ESET 公司的数据，在 2020 年，针对 Windows 远程桌面协议（RDP）的攻击增长了 768%。考虑到疫情期间远程工作的人数大量增加，这并不令人感到意外。

当企业开始提供公共 RDP 服务时，黑客就注意到了。一些 DDoS 攻击利用 RDP 服务器来增强攻击效果，诸如 Trickbot 之类的恶意软件则利用扫描程序来识别易受攻击的开放 RDP 端口。

在远程访问方面，RDP 功能丰富且非常有用。RDP 本身并不危险，但是考虑到它的复杂性、普遍性以及在操作系统中的位置，它就有很大的攻击面了。如果 RDP 的漏洞被暴露，就可能会被黑客利用，从而对企业造成严重的损害。

企业应妥善保护其 RDP 服务，且不应提供对 RDP 服务器的直接访问。反之，企业应提供有限的访问权限，而且要对访问进行保护，以防止攻击者获得管理员级别的访问权限。

公共 RDP 的问题

鉴于 RDP 服务自身的性质，它必须以足够的权限运行，才能以另一用户（包括管理员）的身份操作计算机。如果网络罪犯能够利用服务的漏洞且能够执行任意代码，则其代码可以继承这些权限。

像任何复杂的软件一样，RDP 也存在漏洞，迄今为止最广为人知的漏洞出现在 2019 年。这些漏洞是 BlueKeep（CVE-2019-0708）和 DejaBlue（CVE-2019-1181 和 CVE-2019-1182），攻击者利用这些漏洞执行堆破坏，以绕过授权层并在服务器上执行代码。

微软很快发布了补丁。需要注意的是，在应用补丁解决这些问题时，企业 IT 部门的主要关注点应该是防范未知漏洞。这是因为，新的漏洞会不断出现，而微软无法随时提供补丁。企业必须设计一个能够减轻将来漏洞的系统。

防御性 RDP 设计

设计 RDP 服务时，企业应遵循以下两个原则，这些原则可以限制攻击者利用未知漏洞

的程度。

- 纵深防御：安全应依赖于多层独立的保护服务，而非单个故障点。
- 最低权限原则：仅应向服务和用户授予必需的权限。如果可以，应将任务划分为多个服务，以减少授权服务的范围。

授权应该由其他服务独立执行，而非仅由 RDP 服务器执行。用户只有经过身份验证和授权后，才能访问 RDP 服务。这意味着，RDP 应该部署在安全网关之后，该网关是访问 RDP 服务的唯一通道。用户通过身份验证后，网关仅应向其提供对所需资产的访问。同样，企业应严格限制授予网关和其他公共访问服务的权限。这样一来，即使攻击者能够成功地执行攻击，也无法获得管理员权限。

企业有时会部署 VPN 来解决这一问题。这是一种保护 RDP 的短期方法，但是却存在重大的长期缺陷。企业使用 VPN 提供对专用网络的常规访问，会导致用户得以访问更机密的网络，这违反了最低权限原则。

此外，VPN 很难进行管理和扩展。即使疫情期间的“禁足令”被解除，许多员工仍将保持远程工作状态，因此企业应尽快解决这一问题。

将 RDP 部署在安全的专用网关之后，企业可以配置网络防火墙。这样一来，外部用户只能通过网关进行访问。同样，企业应锁定网络上所有启用 RDP 的计算机，要求用户只能通过网关对其进行访问。从而确保，对一台计算机的未授权访问不会导致对网络上其他计算机的访问。

在新的远程工作环境中，RDP 将继续在实现对虚拟和物理企业计算机的远程访问方面发挥关键作用。通过一些相对简单的措施（及时打补丁、将 RDP 部署在安全网关之后，以及采用最低权限原则），企业可以安全地提供远程访问，不必担心会为黑客提供新的漏洞。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com