Microsoft Windows RDP 远程桌面服务多个远程代码执行漏洞通告

文档信息

编号	QianxinTI-SV-2019-0015
关键字	Windows Remote Desktop Services RDPCVE-2019-1181/CVE-2019-1182/CVE-2019-1222/CVE-2019-1226
发布日期	2019 年 08 月 13 日
更新日期	2019 年 08 月 14 日
TLP	WHITE
分析团队	奇安信威胁情报中心红雨滴团队

通告背景

2019 年 8 月 13 日，微软发布了 8 月例行补丁更新列表，其中包含四个威胁评级为严重的 RDP（远程桌面服务）远程代码执行漏洞。攻击者可以通过构造恶意特殊的 RDP 请求触发漏洞，获取在目标系统上的远程代码执行权限。需要注意的是从微软公告中来看，该漏洞为预身份验证，即无需用户交互（即利用的要求可能较低），这意味着该漏洞有可能被蠕虫所利用，其中漏洞 CVE-2019-1181/CVE-2019-1182 是微软在升级加固远程桌面服务期间所发现。目前，没有证据表明任何第三方都知道这两个漏洞的存在，但随着漏洞补丁的发布技术细节极有可能被包括攻击者在内的第三方所分析了解。

奇安信威胁情报中心红雨滴团队第一时间跟进了这些漏洞，从目前来看该漏洞主要影响 Windows 主流操作系统(详见漏洞概要)，而 Windows XP、Windows Server 2003 和 Windows Server 2008 不受影响，远程桌面协议(RDP)本身也不受影响，鉴于微软给出的严重级别评级及之前类似漏洞经验，强烈建议用户立即进行补丁更新处理。

从下图可见，四个漏洞的 CVSS 评级均高达 9.8 分，可见严重性极大。

漏洞概要

漏洞名称	Microsoft Windows Remote Desktop Services 远程代码执行漏洞

威胁类型	远程代码执行	威胁等级	严重	漏洞 ID	CVE-2019-1181 CVE-2019-1182 CVE-2019-1222 CVE-2019-1226
利用场景	未经身份验证的攻击者可以通过发送特殊构造的数据包触发，可导致远程代码执行控制用户系统。				
受影响系统及应用版本					
Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 所有 Windows 10 版本和服务器版本。					

漏洞描述

漏洞为四处存在于 Windows Remote Desktop Services（远程桌面服务）中的远程代码执行漏洞，目前技术细节未知。

影响面评估

目前网络上开放 RDP 服务的服务器数量巨大，影响面极大。

处置建议

修复方法

1. 目前软件厂商微软已经发布了漏洞相应的补丁，奇安信威胁情报中心建议进行相关升级
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226
2. 如暂时无法更新补丁，可以通过在系统上启用网络及身份认证（NLA）以暂时规避该漏洞影响（需要注意以下三条只对 CVE-2019-1181/CVE-2019-1182 有效）。
3. 在企业外围防火墙阻断 TCP 端口 3389 的链接
4. 如无需求，可禁用相关远程桌面服务

参考资料

https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226