关于 Windows 远程桌面服务远程代码执行漏洞的预警（重要）

日前，编号为 CVE-2019-0708 的 Windows 远程桌面服务（RDP）远程代码执行漏洞利用代码（EXP）已公开。近日，微软再一次发布危害相似漏洞的安全更新补丁，修复了 4 个远程桌面服务远程代码执行漏洞，CVE 编号分别为：CVE-2019-1181、CVE-2019-1182、CVE-2019-1222、CVE-2019-1226。

值此网络安全重点保障时期，请各单位、全校师生尽快修复漏洞！

上述 4 个漏洞影响的产品版本包括：

Windows 10 for 32-bit Systems

Windows 10 for x64-based Systems

Windows 10 Version 1607 for 32-bit Systems

Windows 10 Version 1607 for x64-basedSystems

Windows 10 Version 1703 for 32-bit Systems

Windows 10 Version 1703 for x64-basedSystems

Windows 10 Version 1709 for 32-bit Systems

Windows 10 Version 1709 for 64-basedSystems

Windows 10 Version 1709 for ARM64-based Systems

Windows 10 Version 1803 for 32-bit Systems

Windows 10 Version 1803 for ARM64-basedSystems

Windows 10 Version 1803 for x64-basedSystems

Windows 10 Version 1809 for 32-bit Systems

Windows 10 Version 1809 for ARM64-basedSystems

Windows 10 Version 1809 for x64-basedSystems

Windows 10 Version 1903 for 32-bit Systems

Windows 10 Version 1903 for ARM64-basedSystems

Windows 10 Version 1903 for x64-basedSystems

Windows 7 for 32-bit Systems Service Pack 1

Windows 7 for x64-based Systems ServicePack 1

Windows 8.1 for 32-bit systems

Windows 8.1 for x64-based systems

Windows RT 8.1

Windows Server 2008 R2 for tanium-BasedSystems Service Pack 1

Windows Server 2008 R2 for x64-basedSystems Service Pack 1

Windows Server 2008 R2 for x64-basedSystems Service Pack 1 (Server Core installation)

Windows Server 2012

Windows Server 2012 (Server Coreinstallation)

Windows Server 2012 R2

Windows Server 2012 R2 (Server Coreinstallation)

Windows Server 2016

Windows Server 2016 (Server Coreinstallation)

Windows Server 2019

Windows Server 2019 (Server Coreinstallation)

Windows Server, version 1803 (Server CoreInstallation)

Windows Server, version 1903 (Server Coreinstallation)

漏洞处置建议如下：

1. 官方补丁链接如下：

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. 另可采取下列临时防护措施：

1) 禁用远程桌面服务。

2) 通过主机防火墙对远程桌面服务端口进行阻断(默认为 TCP 3389)。

3) 启用网络级认证(NLA),此方案适用于 Windows 7、Windows Server 2008 和 Windows Server 2008 R2。