微软 8 月份月度安全漏洞预警

一、概要

微软近日发布了8月份安全补丁更新，共披露了121个漏洞，其中17个漏洞标记为Critical漏洞，103个标记为Important漏洞（2个0 day漏洞），1个标记为Moderate漏洞，可导致信息泄露、执行远程代码、权限提升、功能绕过、拒绝服务等影响。主要涉及以下产品/组件：Microsoft Windows、Microsoft Defender、Defender for Endpoint、Microsoft Dynamics、Exchange Server、Office、SharePoint Server等组件

微软官方说明：https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

二、漏洞级别

漏洞级别：【严重】

（说明：漏洞级别共四级：一般、重要、严重、紧急。）

三、影响范围

Microsoft Windows、Microsoft Defender、Defender for Endpoint、Microsoft Dynamics、Exchange Server、Office、SharePoint Server等多个产品和组件。

四、严重漏洞说明详情

CVE编号	漏洞名称	标签	严重程度
CVE-2022-30133	Windows 点对点协议(PPP) 远程代码执行漏洞	Windows Point-to-Point Tunneling	Critical

		Protocol	
CVE-2022-35744	Windows 点对点协议(PPP) 远程代码执行漏洞	Windows Point-to-Point Tunneling Protocol	Critical
CVE-2022-34691	Active Directory 域服务特权提升漏洞	Active Directory Domain Services	Critical
CVE-2022-33646	Azure Batch 节点代理远程代码执行漏洞	Azure Batch Node Agent	Critical
CVE-2022-21980	Microsoft Exchange Server 特权提升漏洞	Microsoft Exchange Server	Critical
CVE-2022-24477	Microsoft Exchange Server 特权提升漏洞	Microsoft Exchange Server	Critical
CVE-2022-24516	Microsoft Exchange Server 特权提升漏洞	Microsoft Exchange Server	Critical
CVE-2022-35752	RAS点对点隧道协议远程代码执行漏洞	Remote Access Service Point-to-Point Tunneling Protocol	Critical
CVE-2022-35753	RAS点对点隧道协议远程代码执行漏洞	Remote Access Service Point-to-	Critical

		Point Tunneling Protocol	
CVE-2022-35804	SMB 客户端和服务器远程代码执行漏洞	Windows Kernel	Critical
CVE-2022-34696	Windows Hyper-V 远程执行代码漏洞	Role: Windows Hyper-V	Critical
CVE-2022-34702	Windows 安全套接字隧道协议 (SSTP) 远程代码执行漏洞	Windows Secure Socket Tunneling Protocol (SSTP)	Critical
CVE-2022-34714	Windows 安全套接字隧道协议 (SSTP) 远程代码执行漏洞	Windows Secure Socket Tunneling Protocol (SSTP)	Critical
CVE-2022-35745	Windows 安全套接字隧道协议 (SSTP) 远程代码执行漏洞	Windows Secure Socket Tunneling Protocol (SSTP)	Critical
CVE-2022-35766	Windows 安全套接字隧道协议 (SSTP) 远程代码执行漏洞	Windows Secure Socket Tunneling Protocol (SSTP)	Critical
CVE-2022-35767	Windows 安全套接字隧道协议 (SSTP) 远程代码执行漏洞	Windows Secure Socket Tunneling Protocol (SSTP)	Critical

CVE-2022-35794	Windows 安全套接字隧道协议 (SSTP) 远程代码执行漏洞	Windows Secure Socket Tunneling Protocol (SSTP)	Critical

（注：以上为微软Critical漏洞，其他漏洞及详情请参见微软官方说明）

五、安全建议

1、可通过Windows Update自动更新微软补丁修复漏洞，也可以手动下载补丁，补丁下载地址：

https://msrc.microsoft.com/update-guide/

2、为确保数据安全，建议重要业务数据进行异地备份。

注意：修复漏洞前请将数据和资料**备份**，并进行充分测试。

中国政务云SRE共享中心-安全运营中心

2022年8月16日