微软 4 月份月度安全漏洞预警

一、概要

微软近日发布了4月份安全补丁更新，共披露了97个漏洞，其中7个漏洞标记为Critical漏洞，90个标记为Important漏洞，可导致远程代码执行、权限提升、敏感信息泄露等影响。主要涉及以下产品/组件：Microsoft Windows and Windows Components; Office and Office Components; Windows Defender; SharePoint Server; Windows Hyper-V; PostScript Printer; Microsoft Dynamics等多个产品和组件。

微软官方说明： https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr

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 and Windows Components; Office and Office Components; Windows Defender; SharePoint Server; Windows Hyper-V; PostScript Printer; Microsoft Dynamics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-2023-28231	DHCP 服务器服务远程代码执行 脆弱性	Windows DHCP Server	Critical
CVE-2023-28219	第 2 层隧道协议远程代码 执行漏洞	Windows Layer 2 Tunneling Protocol	Critical
CVE-2023-28220	第 2 层隧道协议远程代码 执行漏洞	Windows Layer 2 Tunneling Protocol	Critical
CVE-2023-21554	微软消息队列远程代码 执行漏洞	Microsoft Message Queuing	Critical
CVE-2023-28291	原始图像扩展远程代码执行 脆弱性	Windows Raw Image Extension	Critical
CVE-2023-28232	窗口点对点隧道协议 远程执行代码漏洞	Windows Point-to-Point Tunneling Protocol	Critical

CVE-2023-28250	Windows Pragmatic General Multicast （PGM） 远程执行代码漏洞	Windows PGM	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。

基地云SRE团队-安全运营中心

2023年4月13日