

微软官方发布了7月安全更新公告，包含了Windows Hyper-V、Microsoft Office、Win32k、Windows Graphics Component、Kernel Streaming WOW Thunk Service Driver和Microsoft Windows Codecs Library等微软家族多个软件的安全更新补丁。请相关用户及时更新对应补丁修复漏洞。

## 一、漏洞信息

微软（Microsoft）是一家美国跨国科技企业，以研发、制造、授权和提供广泛的电脑软件服务业务为主。最为著名和畅销的产品为Windows操作系统和Office系列软件，是全球最大的电脑软件提供商，每月微软会更新安全补丁用于用户及时更新漏洞信息。

### 漏洞速览表

1.本月存在6个在野0day漏洞，经研判，需要重点关注的0day漏洞如下：

- Windows内核特权提升漏洞（CVE-2024-38106）
- 脚本引擎内存损坏漏洞（CVE-2024-38178）
- Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38193）

2.本月披露漏洞中，被利用可能性较高的漏洞如下：

- Windows TCP/IP 远程代码执行漏洞（CVE-2024-38063）
- Windows内核特权提升漏洞（CVE-2024-38106）
- Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38141）
- 脚本引擎内存损坏漏洞（CVE-2024-38178）
- Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38193）
- Windows Common Log File System Driver特权提升漏洞（CVE-2024-38196）
- Kernel Streaming WOW Thunk 服务驱动程序特权提升漏洞（CVE-2024-38125）
- Kernel Streaming WOW Thunk 服务驱动程序特权提升漏洞（CVE-2024-38144）
- Microsoft DWM 核心库特权提升漏洞（CVE-2024-38147）
- Windows Secure Channel拒绝服务漏洞（CVE-2024-38148）
- Windows DWM 核心库特权提升漏洞（CVE-2024-38150）

3.本月披露漏洞中较为高危的漏洞如下：

- Azure Stack Hub 欺骗漏洞（CVE-2024-38108）
- Azure Health Bot 特权提升漏洞（CVE-2024-38109）
- Windows TCP/IP 远程代码执行漏洞（CVE-2024-38063）
- Windows Reliable Multicast Transport Driver (RMCAT)远程代码执行漏洞（CVE-2024-38140）
- Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38141）
- Windows Network Virtualization远程代码执行漏洞（CVE-2024-38159）
- Windows Network Virtualization远程代码执行漏洞（CVE-2024-38160）
- Windows Line Printer Daemon (LPD)服务远程代码执行漏洞（CVE-2024-38199）
- Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38193）

### 漏洞详情

#### 1.Windows内核特权提升漏洞（CVE-2024-38106）

漏洞标题	Windows内核特权提升漏洞（CVE-2024-38106）
------	---------------------------------

漏洞类型	权限提升
影响目标	
影响主体	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-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
漏洞编号	
CVE编号	CVE-2024-38106
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7
危害等级	高危
CVSS向量	
访问途径 (AV)	本地
攻击复杂度 (AC)	高
所需权限 (PR)	低

用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高

2.脚本引擎内存损坏漏洞（CVE-2024-38178）

漏洞标题	脚本引擎内存损坏漏洞（CVE-2024-38178）
漏洞类型	远程代码执行
影响目标	
影响主体	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-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)

漏洞编号	
CVE编号	CVE-2024-38178
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.5
危害等级	高危
CVSS向量	
访问途径（AV）	网络
攻击复杂度（AC）	低
所需权限（PR）	无需任何权限
用户交互（UI）	需要用户交互
影响范围（S）	不变
机密性影响（C）	高
完整性影响（I）	高
可用性影响（A）	高

3.Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38193）

漏洞标题	Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38193）
漏洞类型	权限提升
影响目标	

影响主体	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-based Systems
	Windows 10 Version 1809 for 32-bit Systems
	Windows 10 Version 1809 for ARM64-based Systems
	Windows 10 Version 1809 for x64-based Systems
	Windows 10 Version 21H2 for 32-bit Systems
	Windows 10 Version 21H2 for ARM64-based Systems
	Windows 10 Version 21H2 for x64-based Systems
	Windows 10 Version 22H2 for 32-bit Systems
	Windows 10 Version 22H2 for ARM64-based Systems
	Windows 10 Version 22H2 for x64-based Systems
	Windows 11 version 21H2 for ARM64-based Systems
	Windows 11 version 21H2 for x64-based Systems
	Windows 11 Version 22H2 for ARM64-based Systems
	Windows 11 Version 22H2 for x64-based Systems
	Windows 11 Version 23H2 for ARM64-based Systems
	Windows 11 Version 23H2 for x64-based Systems
	Windows 11 Version 24H2 for ARM64-based Systems
	Windows 11 Version 24H2 for x64-based Systems
	Windows Server 2012 R2
	Windows Server 2012 R2 (Server Core installation)
	Windows Server 2016
	Windows Server 2016 (Server Core installation)
	Windows Server 2019
	Windows Server 2019 (Server Core installation)
	Windows Server 2022
	Windows Server 2022 (Server Core installation)
	Windows Server 2022, 23H2 Edition (Server Core installation)
漏洞编号	
CVE编号	CVE-2024-38193
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.8
危害等级	高危
CVSS向量	
访问途径 (AV)	本地
攻击复杂度 (AC)	低
所需权限 (PR)	低

用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高

4.Windows TCP/IP 远程代码执行漏洞 (CVE-2024-38063)

漏洞标题	Windows TCP/IP 远程代码执行漏洞 (CVE-2024-38063)
漏洞类型	远程代码执行
影响目标	

影响主体	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-based Systems
	Windows 10 Version 1809 for 32-bit Systems
	Windows 10 Version 1809 for ARM64-based Systems
	Windows 10 Version 1809 for x64-based Systems
	Windows 10 Version 21H2 for 32-bit Systems
	Windows 10 Version 21H2 for ARM64-based Systems
	Windows 10 Version 21H2 for x64-based Systems
	Windows 10 Version 22H2 for 32-bit Systems
	Windows 10 Version 22H2 for ARM64-based Systems
	Windows 10 Version 22H2 for x64-based Systems
	Windows 11 version 21H2 for ARM64-based Systems
	Windows 11 version 21H2 for x64-based Systems
	Windows 11 Version 22H2 for ARM64-based Systems
	Windows 11 Version 22H2 for x64-based Systems
	Windows 11 Version 23H2 for ARM64-based Systems
	Windows 11 Version 23H2 for x64-based Systems
	Windows 11 Version 24H2 for ARM64-based Systems
	Windows 11 Version 24H2 for x64-based Systems
	Windows Server 2008 for 32-bit Systems Service Pack 2
	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
	Windows Server 2008 for x64-based Systems Service Pack 2
	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
	Windows Server 2008 R2 for x64-based Systems Service Pack 1
	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
	Windows Server 2012
	Windows Server 2012 (Server Core installation)
	Windows Server 2012 R2
	Windows Server 2012 R2 (Server Core installation)
	Windows Server 2016
	Windows Server 2016 (Server Core installation)
	Windows Server 2019
	Windows Server 2019 (Server Core installation)
	Windows Server 2022
	Windows Server 2022 (Server Core installation)
	Windows Server 2022, 23H2 Edition (Server Core installation)
漏洞编号	
CVE编号	CVE-2024-38063
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	9.8

危害等级	严重
CVSS向量	
访问途径（AV）	网络
攻击复杂度（AC）	低
所需权限（PR）	无需任何权限
用户交互（UI）	不需要用户交互
影响范围（S）	不变
机密性影响（C）	高
完整性影响（I）	高
可用性影响（A）	高

5.Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38141）

漏洞标题	Windows Ancillary Function Driver for WinSock特权提升漏洞（CVE-2024-38141）
漏洞类型	权限提升
影响目标	



影响主体	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-based Systems
	Windows 10 Version 1809 for 32-bit Systems
	Windows 10 Version 1809 for ARM64-based Systems
	Windows 10 Version 1809 for x64-based Systems
	Windows 10 Version 21H2 for 32-bit Systems
	Windows 10 Version 21H2 for ARM64-based Systems
	Windows 10 Version 21H2 for x64-based Systems
	Windows 10 Version 22H2 for 32-bit Systems
	Windows 10 Version 22H2 for ARM64-based Systems
	Windows 10 Version 22H2 for x64-based Systems
	Windows 11 version 21H2 for ARM64-based Systems
	Windows 11 version 21H2 for x64-based Systems
	Windows 11 Version 22H2 for ARM64-based Systems
	Windows 11 Version 22H2 for x64-based Systems
	Windows 11 Version 23H2 for ARM64-based Systems
	Windows 11 Version 23H2 for x64-based Systems
	Windows 11 Version 24H2 for ARM64-based Systems
	Windows 11 Version 24H2 for x64-based Systems
	Windows Server 2012
	Windows Server 2012 (Server Core installation)
	Windows Server 2012 R2
	Windows Server 2012 R2 (Server Core installation)
	Windows Server 2016
	Windows Server 2016 (Server Core installation)
	Windows Server 2019
	Windows Server 2019 (Server Core installation)
	Windows Server 2022
	Windows Server 2022 (Server Core installation)
	Windows Server 2022, 23H2 Edition (Server Core installation)
漏洞编号	
CVE编号	CVE-2024-38141
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.8
危害等级	高危
CVSS向量	
访问途径 (AV)	本地
攻击复杂度 (AC)	低

所需权限 (PR)	低
用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高

6.Windows Common Log File System Driver特权提升漏洞 (CVE-2024-38196)

漏洞标题	Windows Common Log File System Driver特权提升漏洞 (CVE-2024-38196)
漏洞类型	权限提升
影响目标	

影响主体	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-based Systems
	Windows 10 Version 1809 for 32-bit Systems
	Windows 10 Version 1809 for ARM64-based Systems
	Windows 10 Version 1809 for x64-based Systems
	Windows 10 Version 21H2 for 32-bit Systems
	Windows 10 Version 21H2 for ARM64-based Systems
	Windows 10 Version 21H2 for x64-based Systems
	Windows 10 Version 22H2 for 32-bit Systems
	Windows 10 Version 22H2 for ARM64-based Systems
	Windows 10 Version 22H2 for x64-based Systems
	Windows 11 version 21H2 for ARM64-based Systems
	Windows 11 version 21H2 for x64-based Systems
	Windows 11 Version 22H2 for ARM64-based Systems
	Windows 11 Version 22H2 for x64-based Systems
	Windows 11 Version 23H2 for ARM64-based Systems
	Windows 11 Version 23H2 for x64-based Systems
	Windows 11 Version 24H2 for ARM64-based Systems
	Windows 11 Version 24H2 for x64-based Systems
	Windows Server 2008 for 32-bit Systems Service Pack 2
	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
	Windows Server 2008 for x64-based Systems Service Pack 2
	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
	Windows Server 2008 R2 for x64-based Systems Service Pack 1
	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
	Windows Server 2012
	Windows Server 2012 (Server Core installation)
	Windows Server 2012 R2
	Windows Server 2012 R2 (Server Core installation)
	Windows Server 2016
	Windows Server 2016 (Server Core installation)
	Windows Server 2019
	Windows Server 2019 (Server Core installation)
	Windows Server 2022
	Windows Server 2022 (Server Core installation)
	Windows Server 2022, 23H2 Edition (Server Core installation)
漏洞编号	
CVE编号	CVE-2024-38196
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.8

危害等级	高危
CVSS向量	
访问途径（AV）	本地
攻击复杂度（AC）	低
所需权限（PR）	低
用户交互（UI）	不需要用户交互
影响范围（S）	不变
机密性影响（C）	高
完整性影响（I）	高
可用性影响（A）	高
威胁状态	

7.Kernel Streaming WOW Thunk 服务驱动程序特权提升漏洞（CVE-2024-38125）

漏洞标题	Kernel Streaming WOW Thunk 服务驱动程序特权提升漏洞（CVE-2024-38125）
漏洞类型	权限提升
影响目标	

影响主体	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-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
	漏洞编号
	CVE编号
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.8

危害等级	高危
CVSS向量	
访问途径（AV）	本地
攻击复杂度（AC）	低
所需权限（PR）	低
用户交互（UI）	不需要用户交互
影响范围（S）	不变
机密性影响（C）	高
完整性影响（I）	高
可用性影响（A）	高

8. Kernel Streaming WOW Thunk 服务驱动程序特权提升漏洞（CVE-2024-38144）

漏洞标题	Kernel Streaming WOW Thunk 服务驱动程序特权提升漏洞（CVE-2024-38144）
漏洞类型	权限提升
影响目标	

影响主体	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-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
	漏洞编号
	CVE编号
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	8.8

危害等级	高危
CVSS向量	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	低
用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高
威胁状态	

9.Microsoft DWM 核心库特权提升漏洞 (CVE-2024-38147)

漏洞标题	Microsoft DWM 核心库特权提升漏洞 (CVE-2024-38147)
漏洞类型	权限提升
影响目标	
影响主体	Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
漏洞编号	
CVE编号	CVE-2024-38147



CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.8
危害等级	高危
<b>CVSS向量</b>	
访问途径 (AV)	本地
攻击复杂度 (AC)	低
所需权限 (PR)	低
用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高

10.Windows Secure Channel拒绝服务漏洞 (CVE-2024-38148)

漏洞标题	Windows Secure Channel拒绝服务漏洞 (CVE-2024-38148)
漏洞类型	拒绝服务
<b>影响目标</b>	
影响主体	Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation) tr>
<b>漏洞编号</b>	
CVE编号	CVE-2024-38148
CNVD编号	未分配
CNNVD编号	未分配

CVSS3.1评分	7.8
危害等级	高危
<b>CVSS向量</b>	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	无需任何权限
用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	无
完整性影响 (I)	无
可用性影响 (A)	高
<b>威胁状态</b>	

11.Windows DWM 核心库特权提升漏洞 (CVE-2024-38150)

漏洞标题	Windows DWM 核心库特权提升漏洞 (CVE-2024-38150)
漏洞类型	权限提升
<b>影响目标</b>	
影响主体	Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
<b>漏洞编号</b>	
CVE编号	CVE-2024-38150

CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	7.8
危害等级	高危
<b>CVSS向量</b>	
访问途径（AV）	本地
攻击复杂度（AC）	低
所需权限（PR）	低
用户交互（UI）	不需要用户交互
影响范围（S）	不变
机密性影响（C）	高
完整性影响（I）	高
可用性影响（A）	高

12.Azure Stack Hub 欺骗漏洞（CVE-2024-38108）

漏洞标题	Azure Stack Hub 欺骗漏洞（CVE-2024-38108）
漏洞描述	Azure Stack Hub 是微软提供的一种混合云平台，它允许企业在自己的数据中心内运行 Azure 服务。Azure Stack Hub 存在身份欺骗漏洞，未经身份验证的攻击者可以通过诱导受害者在虚拟机的网页浏览器中加载恶意代码来利用此漏洞，从而使攻击者能够利用虚拟机的隐式身份。
<b>漏洞编号</b>	
CVE编号	CVE-2024-38108
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	9.3
危害等级	严重
<b>CVSS向量</b>	
访问途径（AV）	网络

攻击复杂度 (AC)	低
所需权限 (PR)	无需任何权限
用户交互 (UI)	需要用户交互
影响范围 (S)	改变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	无
参考链接	
<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38108">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38108</a>	

13.Windows Network Virtualization远程代码执行漏洞（CVE-2024-38159）

漏洞标题	Windows Network Virtualization远程代码执行漏洞（CVE-2024-38159）
漏洞描述	Windows Network Virtualization 中存在远程代码执行漏洞，具备较高权限的攻击者可利用该漏洞实现 guest-to-host 逃逸。
漏洞编号	
CVE编号	CVE-2024-38159
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	9.1
危害等级	严重
CVSS向量	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	高

用户交互 (UI)	不需要用户交互
影响范围 (S)	改变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高
参考链接	
	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38159">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38159</a>

14.Windows Network Virtualization远程代码执行漏洞（CVE-2024-38160）

漏洞标题	Windows Network Virtualization远程代码执行漏洞（CVE-2024-38160）
漏洞描述	Windows Network Virtualization 中存在远程代码执行漏洞，具备较高权限的攻击者可利用该漏洞实现 guest-to-host 逃逸。
漏洞编号	
CVE编号	CVE-2024-38160
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	9.1
危害等级	严重
CVSS向量	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	高
用户交互 (UI)	不需要用户交互
影响范围 (S)	改变

机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高
参考链接	
	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38160">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38160</a>

15.Windows Line Printer Daemon (LPD)服务远程代码执行漏洞（CVE-2024-38199）

漏洞标题	Windows Line Printer Daemon (LPD)服务远程代码执行漏洞（CVE-2024-38199）
漏洞描述	Windows Line Printer Daemon Service 是 Windows 操作系统中的一个网络服务，它使用 Line Printer Remote (LPR)/Line Printer Daemon (LPD) 协议来处理网络打印任务，支持 Unix/Linux 系统与 Windows 系统之间的跨平台打印。本次漏洞发生在 LPD 协议中，未通过身份验证的攻击者可通过网络向存在漏洞的 Windows Line Printer Daemon Service 发送特制的打印任务。成功利用该漏洞可在服务器上远程执行代码。
漏洞编号	
CVE编号	CVE-2024-38199
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1 评分	9.8
危害等级	严重
CVSS向量	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	无需任何权限
用户交互 (UI)	不需要用户交互

影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高
参考链接	
	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38199">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38199</a>

16.Windows Reliable Multicast Transport Driver (RMCAST)远程代码执行漏洞（CVE-2024-38140）

漏洞标题	Windows Reliable Multicast Transport Driver (RMCAST)远程代码执行漏洞（CVE-2024-38140）
漏洞描述	Windows Reliable Multicast Transport Driver (RMCAST) 是 Windows 操作系统中的一种网络驱动程序，它用于支持可靠的多播传输。未经身份验证的攻击者可通过 socket 向服务器上的 Windows Pragmatic General Multicast (PGM) 发送特制数据包来利用该漏洞，实现远程代码执行，且用户无需进行任何交互。
漏洞编号	
CVE编号	CVE-2024-38140
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1 评分	9.8
危害等级	严重
CVSS向量	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	无需任何权限

用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高
参考链接	
	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38140">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38140</a>

17.Azure Health Bot 特权提升漏洞 (CVE-2024-38109)

漏洞标题	Azure Health Bot 特权提升漏洞 (CVE-2024-38109)
漏洞描述	Azure Health Bot 是 Microsoft 提供的一个基于云的服务，专门为医疗领域设计，用于创建和部署 AI 驱动的聊天机器人。Azure Health Bot 服务存在权限提升漏洞，经过身份验证的攻击者可利用 Azure Health Bot 服务端的 SSRF 漏洞，通过网络提升权限。
漏洞编号	
CVE编号	CVE-2024-38109
CNVD编号	未分配
CNNVD编号	未分配
CVSS3.1评分	9.8
危害等级	严重
CVSS向量	
访问途径 (AV)	网络
攻击复杂度 (AC)	低
所需权限 (PR)	无需任何权限



用户交互 (UI)	不需要用户交互
影响范围 (S)	不变
机密性影响 (C)	高
完整性影响 (I)	高
可用性影响 (A)	高
参考链接	
	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38109">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38109</a>

## 二、修复方案

**官方修复方案:**

目前微软针对支持的产品已发布升级补丁修复了上述漏洞，请用户参考官方通告及时下载更新补丁。

补丁获取:

<https://msrc.microsoft.com/update-guide/vulnerability>

Windows 更新:

自动更新:

Microsoft Update默认启用，当系统检测到可用更新时，将会自动下载更新并在下一次启动时安装。

手动更新:

- 1、点击“开始菜单”或按Windows快捷键，点击进入“设置”。
- 2、选择“更新和安全”，进入“Windows更新”（Windows 8、Windows 8.1、Windows Server 2012以及Windows Server 2012 R2可通过控制面板进入“Windows更新”，具体步骤为“控制面板”->“系统和安全”->“Windows更新”）。
- 3、选择“检查更新”，等待系统将自动检查并下载可用更新。
- 4、重启计算机，安装更新系统重新启动后，可通过进入“Windows更新”->“查看更新历史记录”查看是否成功安装了更新。

## 三、参考资料

<https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug>