微软 1 月安全更新多个产品高危漏洞通告

■ **通告编号**	**NS-2024-01**	■ 发布日期	**2024-01-10**
■ **漏洞危害**	**攻击者利用本次安全更新中的漏洞，可造成信息泄露、权限提升、远程代码执行等。**		
■ **TAG**	安全更新、Microsoft Exchange Server、Microsoft Office、Windows Kernel		

一. 漏洞概述

1 月 10 日，绿盟科技 CERT 监测到微软发布 1 月安全更新补丁，修复了 49 个安全问题，涉及 Windows、Microsoft Office、Microsoft SQL Server、Microsoft Visual Studio 等广泛使用的产品，其中包括安全功能绕过漏洞、远程代码执行漏洞等高危漏洞类型。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞有 2 个，重要（Important）漏洞有 47 个，请相关用户尽快更新补丁进行防护，完整漏洞列表请参考附录。

参考链接：

https://msrc.microsoft.com/update-guide/releaseNote/2024-Jan

二. 重点漏洞简述

根据产品流行度和漏洞重要性筛选出此次更新中包含影响较大的漏洞，请相关用户重点进行关注：

Windows Kerberos 安全功能绕过漏洞(CVE-2024-20674)：

Windows Kerberos 存在一个安全功能绕过漏洞(CVE-2024-20674)，经过身份认证的相邻攻击者可以通过建立中间人攻击（MITM）或其他本地网络欺骗技术来利用此漏洞，然后向受害者主机发送恶意的 Kerberos 消息以冒充经过 Kerberos 身份验证服务器。CVSS 评分为 9.0。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674

Microsoft 通用日志文件系统权限提升漏洞(CVE-2024-20653):

Microsoft 通用日志文件系统存在一个权限提升漏洞(CVE-2024-20653)，经过普通用户身份认证的本地攻击者通过运行特制的程序来利用此漏洞，可以获得目标系统的 SYSTEM 权限。。CVSS 评分为 7.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20653

Win32k 权限提升漏洞(CVE-2024-20683)：

Windows Win32K 存在一个权限提升漏洞(CVE-2024-20683)，由于应用程序没有在 Win32k 中正确进行安全限制，具有普通用户权限的本地攻击者可以利用该漏洞提升权限至 SYSTEM。CVSS 评分为 7.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683

Windows Hyper-V 远程代码执行漏洞(CVE-2024-20700)：

Windows Hyper-V 中存在一个远程代码执行漏洞(CVE-2024-20700)，该漏洞的是由于 Windows Hyper-V 中的竞争条件造成的，相邻网络上的远程攻击者可以利用条件竞争并在目标系统上执行任意代码。CVSS 评分为 7.5。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700

Windows 内核权限提升漏洞(CVE-2024-20698):

Windows 内核存在一个权限提升漏洞(CVE-2024-20698)，由于未对 Windows 内核正确进行安全限制，经过普通用户身份认证的本地攻击者通过运行特制的程序可以提升权限至 SYSTEM。CVSS 评分为 7.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698

远程桌面客户端远程代码执行漏洞 (CVE-2024-21307)：

Remote Desktop Client 存在一个远程代码执行漏洞 (CVE-2024-21307)，由远程桌面客户端中的竞争条件造成的，当用户发起连接时，未经身份验证的远程攻击者可以利用漏洞在目标系统上执行任意代码。CVSS 评分为 7.5。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307

Microsoft SharePoint Server 远程代码执行漏洞(CVE-2024-21318)：

Microsoft SharePoint Server 存在一个远程代码执行漏洞(CVE-2024-21318)，由于 Microsoft SharePoint Server 对用户提供的输入验证不足，经过身份验证的远程攻击者可以将特制的输入传递给应用程序并在目标系统上执行任意代码。CVSS 评分为 7.5。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318

Windows Cloud Files Mini Filte 驱动程序权限提升漏洞(CVE-2024-21310)：

由于 Win32k 中的应用程序未实行正确的安全限制，由于未对 Windows Cloud Files Mini Filte 驱动程序正确进行安全限制，具有低权限的本地攻击者通过利用该漏洞绕过安全限制，从而在目标系统上提升至 SYSTEM 权限，且无需用户交互。CVSS 评分 7.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310

三. 影响范围

以下为部分重点关注漏洞的受影响产品版本，其他漏洞影响产品范围请参阅官方通告链接。

漏洞编号	受影响产品版本
CVE-2024-20674 CVE-2024-20653 CVE-2024-20683	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems

	Windows 10 for 32-bit Systems Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-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 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
CVE-2024-20700 CVE-2024-20698	Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019

	Windows 10 Version 1809 for x64-based Systems
CVE-2024-21307	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 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)

CVE-2024-21318	Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016
CVE-2024-21310	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 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)

注：官方已停止对 Windows 10 20H2 版本进行维护，请相关用户升级至支持系统。

四. 漏洞防护

4.1 补丁更新

目前微软官方已针对受支持的产品版本发布了修复以上漏洞的安全补丁，强烈建议受影响用户尽快安装补丁进行防护，官方下载链接：

https://msrc.microsoft.com/update-guide/releaseNote/2024-Jan

注：由于网络问题、计算机环境问题等原因，Windows Update 的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。

右键点击 Windows 图标，选择“设置(N)”，选择“更新和安全”-“Windows 更新”，查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

针对未成功安装的更新，可点击更新名称跳转到微软官方下载页面，建议用户点击该页面上的链接，转到“Microsoft 更新目录”网站下载独立程序包并安装。

附录：漏洞列表

影响产品	CVE 编号	漏洞标题	严重程度
Windows	CVE-2024-20674	Windows Kerberos 安全功能绕过漏洞	Critical
Windows	CVE-2024-20700	Windows Hyper-V 远程代码执行漏洞	Critical
Windows	CVE-2024-20666	BitLocker 安全功能绕过漏洞	Important
Microsoft Office	CVE-2024-20677	Microsoft Office 远程代码执行漏洞	Important
Azure	CVE-2024-20676	Azure Storage Mover 远程代码执行漏洞	Important
Windows	CVE-2024-20654	Microsoft ODBC Driver 远程代码执行漏洞	Important
Windows	CVE-2024-20657	Windows Group Policy 权限提升漏洞	Important
Windows	CVE-2024-20658	Microsoft Virtual Hard Disk 权限提升漏洞	Important
Windows	CVE-2024-20680	Windows Message Queuing Client (MSMQC) Information Disclosure	Important
Windows	CVE-2024-20682	Windows Cryptographic Services 远程代码执行漏洞	Important
Windows	CVE-2024-20683	Win32k 权限提升漏洞	Important

Windows	CVE-2024-20690	Windows Nearby Sharing 欺骗漏洞	Important
Windows	CVE-2024-20691	Windows Themes 信息披露漏洞	Important
Windows	CVE-2024-20694	Windows CoreMessaging Information Disclosure Vulnerability	Important
CBL Mariner 1.0 x64,Windows,CBL Mariner 2.0 x64,CBL Mariner 2.0 ARM,CBL Mariner 1.0 ARM	CVE-2022-35737	MITRE: CVE-2022-35737 SQLite allows an array-bounds overflow	Important
Windows	CVE-2024-20696	Windows Libarchive 远程代码执行漏洞	Important
Windows	CVE-2024-20697	Windows Libarchive 远程代码执行漏洞	Important
Windows	CVE-2024-20698	Windows Kernel 权限提升漏洞	Important
Windows	CVE-2024-20699	Windows Hyper-V 拒绝服务漏洞	Important
Windows	CVE-2024-21305	Hypervisor-Protected Code Integrity (HVCI) 安全功能绕过漏洞	Important
Windows	CVE-2024-21307	Remote Desktop Client 远程代码执行漏洞	Important
Windows	CVE-2024-21313	Windows TCP/IP 信息披露漏洞	Important
Windows	CVE-2024-21325	Microsoft Printer Metadata Troubleshooter Tool 远程代码执行漏洞	Important
.NET	CVE-2024-20672	.NET Core and Visual Studio 拒绝服务漏洞	Important

.NET,Microsoft Visual Studio,Microsoft SQL Server,Microsoft .NET Framework,System.Data.SqlClient, Microsoft.Data.SqlClient	CVE-2024-0056	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider 安全功能绕过漏洞	Important
Microsoft Visual Studio,Microsoft .NET Framework,.NET	CVE-2024-0057	NET, .NET Framework, and Visual Studio 安全功能绕过漏洞	Important
Windows	CVE-2024-20652	Windows HTML Platforms 安全功能绕过漏洞	Important
Windows	CVE-2024-20653	Microsoft Common Log File System 权限提升漏洞	Important
Windows	CVE-2024-20655	Microsoft Online Certificate Status Protocol (OCSP) 远程代码执行漏洞	Important
Microsoft Visual Studio	CVE-2024-20656	Visual Studio 权限提升漏洞	Important
Windows	CVE-2024-20660	Microsoft Message Queuing 信息披露漏洞	Important
Windows	CVE-2024-20661	Microsoft Message Queuing 拒绝服务漏洞	Important
Windows	CVE-2024-20662	Windows Online Certificate Status Protocol (OCSP) 信息披露漏洞	Important
Windows	CVE-2024-20663	Windows Message Queuing Client (MSMQC) Information Disclosure	Important
Windows	CVE-2024-20664	Microsoft Message Queuing	Important

		信息披露漏洞	
Windows	CVE-2024-21316	Windows Server Key Distribution Service Security Feature Bypass	Important
Windows	CVE-2024-20681	Windows Subsystem for Linux 权限提升漏洞	Important
Windows	CVE-2024-20686	Win32k 权限提升漏洞	Important
Windows	CVE-2024-20687	Microsoft AllJoyn API 拒绝服务漏洞	Important
Windows	CVE-2024-20692	Microsoft Local Security Authority Subsystem Service 信息披露漏洞	Important
Windows	CVE-2024-21306	Microsoft Bluetooth Driver 欺骗漏洞	Important
Windows	CVE-2024-21309	Windows Kernel-Mode Driver 权限提升漏洞	Important
Windows	CVE-2024-21310	Windows Cloud Files Mini Filter Driver 权限提升漏洞	Important
Windows	CVE-2024-21311	Windows Cryptographic Services 信息披露漏洞	Important
Microsoft .NET Framework	CVE-2024-21312	.NET Framework 拒绝服务漏洞	Important
Windows	CVE-2024-21314	Microsoft Message Queuing 信息披露漏洞	Important
Microsoft Office	CVE-2024-21318	Microsoft SharePoint Server 远程代码执行漏洞	Important
Microsoft Visual Studio,Azure,.NET	CVE-2024-21319	Microsoft Identity Denial of service vulnerability	Important
Windows	CVE-2024-21320	Windows Themes 欺骗漏洞	Important

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。