微软 6 月安全更新多个产品高危漏洞通告

■ **通告编号** **NS-2022-0020**	■ 发布日期 **2022-06-15**
■ **漏洞危害** **攻击者利用本次安全更新中的漏洞，可造成权限提升、远程代码执行等。**	
■ **TAG** 安全更新、Windows、Office、SQL Server	

一. 漏洞概述

6 月 15 日，绿盟科技 CERT 监测到微软发布 6 月安全更新补丁，修复了 55 个安全问题，涉及 Windows、Microsoft Office、SQL Server、.NET framework、HEVC Video Extensions 等广泛使用的产品，其中包括权限提升、远程代码执行等高危漏洞类型。

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 3 个，重要（Important）漏洞有 52 个，其中包括 1 个 0day 漏洞：

Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞（CVE-2022-30190）

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。

绿盟远程安全评估系统（RSAS）已具备微软此次补丁更新中大部分漏洞的检测能力（包括等高危漏洞），请相关用户关注绿盟远程安全评估系统系统插件升级包的更新，及时升级至 V6.0R02F01.2709，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/vulsys

参考链接：

https://msrc.microsoft.com/update-guide/releaseNote/2022-Jun

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：

Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞（CVE-2022-30190）：

MSDT（Microsoft 支持诊断工具）是内置于 Windows 操作系统中的诊断和故障排除工具。本地攻击者可构造恶意的 office 文档利用 Microsoft Word 的远程模板功能获取包含嵌入式 JavaScript 代码的 HTML 文件，该文件利用'ms-msdt' URI 来执行恶意 PowerShell 代码。值得注意的是，该漏洞在宏被禁用的情况下，仍能通过 MSDT（Microsoft Support Diagnostics Tool）功能执行代码，在资源管理器中的预览功能打开的情况下，当恶意文件保存为 RTF 格式时，甚至无需打开文件，通过资源管理器中的预览选项卡即可触发漏洞在目标机器上执行 powershell 代码。该漏洞 PoC 及技术细节已被披露，且已检测到存在在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

Windows Installer 权限提升漏洞（CVE-2022-30147）：

Windows Installer 存在权限提升漏洞，由于 Windows Installer 中的应用程序未实行正确的安全限制，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。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30147

Windows Network File System 远程代码执行漏洞（CVE-2022-30136）：

Windows Network File System 存在远程代码执行漏洞，由于对 Windows Network File System 中用户提供的输入的验证存在缺陷，未经身份验证的远程攻击者可利用该漏洞向目标系统发送特制的 NFS 请求，最终导致在目标系统上任意执行代码，且无需用户交互。CVSS 评分为 9.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136

Windows Advanced Local Procedure Call 权限提升漏洞（CVE-2022-30160）：

Windows Advanced Local Procedure Call 存在权限提升漏洞，由于 Windows Advanced Local Procedure Call 中的应用程序未实行正确的安全限制，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。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30160

Windows Kerberos 权限提升漏洞（CVE-2022-30165）：

Windows Kerberos 存在权限提升漏洞，当网络通过 CredSSP 建立远程凭据保护连接时，经过身份验证的远程攻击者可以利用此漏洞进行权限提升，之后欺骗 Kerberos 进行登录。CVSS 评分为 8.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30165

Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞（CVE-2022-30161）：

未经身份验证的远程攻击者可以通过诱导用户将轻量级目录访问协议 (LDAP) 客户端与恶意 LDAP 服务器相连接，最终导致恶意服务器在 LDAP 客户端中任意执行代码。CVSS 评分为 8.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30161

Windows Hyper-V 远程代码执行漏洞（CVE-2022-30163）：

Windows Hyper-V 是 Microsoft 的本地虚拟机管理程序，具有低权限的远程攻击者可通过在 Hyper-V guest 上运行特制的应用程序，最终导致在 Hyper-V 主机系统执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163

Microsoft SharePoint Server 远程代码执行漏洞（CVE-2022-30157）：

经过身份验证的攻击者通过使用特制的代码创建站点，成功利用漏洞可导致在目标服务器上远程执行代码。在此过程中，攻击者还需要具有在易受攻击的 SharePoint 服务器上创建页面的权限。CVSS 评分为 8.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157

三. 影响范围

以下为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-2022-30190	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 RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 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 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 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems 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-2022-30147	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 RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 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 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 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 Azure Edition Core Hotpatch

	Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems 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-2022-30136	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2019 (Server Core installation) Windows Server 2019
CVE-2022-30160	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 RT 8.1

	Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 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 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 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 Azure Edition Core Hotpatch Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems 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-2022-30165	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 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 Azure Edition Core Hotpatch Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems 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-2022-30161	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 (Serv

	er Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 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 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 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 Azure Edition Core Hotpatch Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems 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-2022-30163	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 8.1 for x64-based systems Windows 7 for x64-based Systems Service Pack 1 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 for x64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 Azure Edition Core Hotpatch Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for x64-based Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for x64-based Systems
CVE-2022-30157	Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2013 Service Pack 1 Microsoft SharePoint Enterprise Server 2016

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/en-us/releaseNote/2022-Jun

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
Role: Windows Hyper-V	CVE-2022-30163	Windows Hyper-V 远程执行代码漏洞	Critical
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30139	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Critical
Windows Network File System	CVE-2022-30136	Windows 网络文件系统远程代码执行漏洞	Critical
.NET and Visual Studio	CVE-2022-30184	.NET 和 Visual Studio 信息泄露漏洞	Important
Azure OMI	CVE-2022-29149	Azure 开放管理基础结构 (OMI) 特权提升漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Azure Real Time Operating System	CVE-2022-30179	Azure RTOS GUIX Studio 远程代码执行漏洞	Important
Azure Real Time Operating System	CVE-2022-30178	Azure RTOS GUIX Studio 远程代码执行漏洞	Important
Azure Real Time Operating System	CVE-2022-30180	Azure RTOS GUIX Studio 信息泄露漏洞	Important
Azure Real Time Operating System	CVE-2022-30177	Azure RTOS GUIX Studio 远程代码执行漏洞	Important
Azure Service Fabric Container	CVE-2022-30137	Azure Service Fabric 容器特权提升漏洞	Important
Intel	CVE-2022-21127	Intel：CVE-2022-21127 特殊寄存器缓冲区数据采样更新（SRBDS 更新）	Important
Intel	CVE-2022-21123	英特尔：CVE-2022-21123 共享缓冲区数据读取 (SBDR)	Important
Intel	CVE-2022-21125	英特尔：CVE-2022-21125 共享缓冲区数据采样 (SBDS)	Important
Intel	CVE-2022-21166	英特尔：CVE-2022-21166 设备寄存器部分写入 (DRPW)	Important
Microsoft Office	CVE-2022-30159	Microsoft Office 信息泄露漏洞	Important
Microsoft Office	CVE-2022-30171	Microsoft Office 信息泄露漏洞	Important
Microsoft Office	CVE-2022-30172	Microsoft Office 信息	Important

影响产品	CVE 编号	漏洞标题	严重程度
		泄露漏洞	
Microsoft Office	CVE-2022-30174	Microsoft Office 远程代码执行漏洞	Important
Microsoft Office Excel	CVE-2022-30173	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office SharePoint	CVE-2022-30158	Microsoft SharePoint Server 远程代码执行漏洞	Important
Microsoft Office SharePoint	CVE-2022-30157	Microsoft SharePoint Server 远程代码执行漏洞	Important
Microsoft Windows ALPC	CVE-2022-30160	Windows 高级本地过程调用特权提升漏洞	Important
Microsoft Windows Codecs Library	CVE-2022-29119	HEVC 视频扩展远程代码执行漏洞	Important
Microsoft Windows Codecs Library	CVE-2022-30188	HEVC 视频扩展远程代码执行漏洞	Important
Microsoft Windows Codecs Library	CVE-2022-30167	AV1 视频扩展远程代码执行漏洞	Important
Microsoft Windows Codecs Library	CVE-2022-30193	AV1 视频扩展远程代码执行漏洞	Important
Microsoft Windows Codecs Library	CVE-2022-29111	HEVC 视频扩展远程代码执行漏洞	Important
Microsoft Windows Codecs Library	CVE-2022-22018	HEVC 视频扩展远程代码执行漏洞	Important
Remote Volume Shadow Copy Service (RVSS)	CVE-2022-30154	Microsoft 文件服务器卷影复制代理服务(RVSS) 特权提升漏洞	Important
SQL Server	CVE-2022-29143	Microsoft SQL Server 远程代码执行漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Windows Ancillary Function Driver for WinSock	CVE-2022-30151	WinSock 特权提升漏洞的 Windows 辅助功能驱动程序	Important
Windows App Store	CVE-2022-30168	Microsoft Photos App 远程代码执行漏洞	Important
Windows Autopilot	CVE-2022-30189	Windows Autopilot 设备管理和注册客户端欺骗漏洞	Important
Windows Container Isolation FS Filter Driver	CVE-2022-30131	Windows 容器隔离 FS 过滤器驱动程序特权提升漏洞	Important
Windows Container Manager Service	CVE-2022-30132	Windows Container Manager 服务特权提升漏洞	Important
Windows Defender	CVE-2022-30150	Windows Defender Remote Credential Guard 特权提升漏洞	Important
Windows Encrypting File System (EFS)	CVE-2022-30145	Windows 加密文件系统 (EFS) 远程代码执行漏洞	Important
Windows File History Service	CVE-2022-30142	Windows 文件历史记录远程执行代码漏洞	Important
Windows Installer	CVE-2022-30147	Windows Installer 特权提升漏洞	Important
Windows iSCSI	CVE-2022-30140	Windows iSCSI 发现服务远程代码执行漏洞	Important
Windows Kerberos	CVE-2022-30164	Kerberos AppContainer 安全功能绕过漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Windows Kerberos	CVE-2022-30165	Windows Kerberos 特权提升漏洞	Important
Windows Kernel	CVE-2022-30162	Windows 内核信息泄露漏洞	Important
Windows Kernel	CVE-2022-30155	Windows 内核拒绝服务漏洞	Important
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30143	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Important
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30161	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Important
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30141	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Important
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30153	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Important
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30149	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Important
Windows LDAP - Lightweight Directory Access Protocol	CVE-2022-30146	Windows 轻量级目录访问协议 (LDAP) 远程代码执行漏洞	Important
Windows Local Security Authority Subsystem Service	CVE-2022-30166	本地安全机构子系统服务提权漏洞	Important
Windows Media	CVE-2022-30135	Windows Media Center 特权提升漏洞	Important
Windows Network Address Translation (NAT)	CVE-2022-30152	Windows 网络地址转换 (NAT) 拒绝服务	Important

影响产品	CVE 编号	漏洞标题	严重程度
		漏洞	
Windows PowerShell	CVE-2022-30148	Windows 所需状态配置 (DSC) 信息泄露漏洞	Important
Windows SMB	CVE-2022-32230	Windows SMB 拒绝服务漏洞	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。