微软 9 月安全更新多个产品高危漏洞通告

■ **通告编号**	**NS-2021-0040**	■ 发布日期	**2021-09-15**
■ **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、Windows、Office、Edge、Visual Studio		

一. 漏洞概述

9 月 15 日，绿盟科技 CERT 监测到微软发布 9 月安全更新补丁，修复了 86 个安全问题，涉及 Windows、Microsoft Office、Microsoft Visual Studio、Azure 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 62 个，中等（Moderate）漏洞有 1 个，其中还包括 9 月初修复的 20 个 Microsoft Edge (Chromium)漏洞。微软针对上周紧急发布的 Microsoft MSHTML 远程代码执行漏洞（CVE-2021-40444）发布了修复补丁，漏洞 EXP 已公开，且监测到在野利用，绿盟科技 CERT 于 9 月 8 日针对此漏洞发布了通告。

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 CVE-2021-36965、CVE-2021-26435、CVE-2021-36952、CVE-2021-26435 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 V6.0R02F01.2408，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/vulsys

参考链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Sep

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：

Open Management Infrastructure 远程代码执行漏洞（CVE-2021-38647）：

开放管理基础设施 (OMI) 是一个开源项目，旨在进一步开发 DMTF CIM/WBEM 标准的生产质量实施。支持大多数的 UNIX 和 Linux 系统发行版，未经身份认证的攻击者可通过 HTTPS 协议发送特制的数据包到目标系统的 OMI 端口（默认为 5986），可实现远程代码执行，CVSS 评分为 9.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647

Microsoft MSHTML 远程代码执行漏洞（CVE-2021-40444）：

MSHTML（又称为 Trident）是微软旗下的 Internet Explorer 浏览器引擎，也用于 Office 应用程序，以在 Word、Excel 或 PowerPoint 文档中呈现 Web 托管的内容。攻击者可通过制作恶意的 ActiveX 控件供托管浏览器呈现引擎的 Microsoft Office 文档使用，成功诱导用户打开恶意文档后，可在目标系统上以该用户权限执行任意代码。漏洞 EXP 已公开，且发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

Windows 脚本引擎内存损坏漏洞漏洞（CVE-2021-26435）

Windows 脚本引擎存在内存损坏漏洞，远程攻击者通过欺骗受害者访问恶意网站或打开特制文件，触发内存损坏从而在目标系统上执行任意代码。CVSS：8.1。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26435

Windows WLAN AutoConfig Service 远程代码执行漏洞（CVE-2021-36965）

相邻网络的攻击者可利用此漏洞实现在目标系统上以 SYSTEM 权限远程代码执行，且不需要用户交互。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36965

Windows Print Spooler 权限提升漏洞（CVE-2021-38671/CVE-2021-38667/CVE-2021-40447）：

Print Spooler 是 Windows 系统中管理打印相关事务的服务，用于管理所有本地和网络打印队列并控制所有打印工作。Windows Print Spooler 中存在多个权限提升漏洞，经过身份认证的本地攻击者利用此类漏洞可在目标系统上提升至 SYSTEM 权限。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38671

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38667

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40447

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-2021-38647	Azure Open Management Infrastructure
CVE-2021-40444 CVE-2021-26435 CVE-2021-36965 CVE-2021-38667 CVE-2021-38671 CVE-2021-40447	Windows Server, version 20H2 (Server Core Installation) Windows Server, version 2004 (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 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 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 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems

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/2021-Sep

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-2021-36965	Windows WLAN AutoConfig Service 远程代码执行漏洞	Critical
Windows	CVE-2021-26435	Windows Scripting Engine 内存泄露漏洞	Critical
Azure	CVE-2021-38647	Open Management Infrastructure 远程代码执行漏洞	Critical
Microsoft Visual Studio	CVE-2021-36952	Visual Studio 远程代码执行漏洞	Important
Windows	CVE-2021-36954	Windows Bind Filter Driver 权限提升漏洞	Important
Windows	CVE-2021-36955	Windows Common Log File System Driver 权限提升漏洞	Important
Windows	CVE-2021-36959	Windows Authenticode 欺骗漏洞	Important
Windows	CVE-2021-36960	Windows SMB 信息披露漏洞	Important
Windows	CVE-2021-36961	Windows Installer 拒绝服务漏洞	Important
Windows	CVE-2021-36962	Windows Installer 信息披露漏洞	Important
Windows	CVE-2021-36963	Windows Common Log File System Driver 权限提升漏洞	Important
Windows	CVE-2021-36964	Windows Event Tracing 权限提升漏洞	Important
Windows	CVE-2021-36966	Windows Subsystem for Linux 权限提升漏洞	Important
Windows	CVE-2021-36967	Windows WLAN AutoConfig	Important

		Service 权限提升漏洞	
Windows	CVE-2021-36968	Windows DNS 权限提升漏洞	Important
Windows	CVE-2021-36969	Windows Redirected Drive Buffering SubSystem Driver 信息披露漏洞	Important
Windows	CVE-2021-36972	Windows SMB 信息披露漏洞	Important
Windows	CVE-2021-36973	Windows Redirected Drive Buffering System 权限提升漏洞	Important
Windows	CVE-2021-36974	Windows SMB 权限提升漏洞	Important
Windows	CVE-2021-36975	Win32k 权限提升漏洞	Important
Microsoft Edge (Chromium-based)	CVE-2021-26436	Microsoft Edge (Chromium-based) 权限提升漏洞	Important
Windows	CVE-2021-38624	Windows Key Storage Provider 安全功能绕过漏洞	Important
Windows	CVE-2021-38625	Windows Kernel 权限提升漏洞	Important
Windows	CVE-2021-38626	Windows Kernel 权限提升漏洞	Important
Windows	CVE-2021-38628	Windows Ancillary Function Driver for WinSock 权限提升漏洞	Important
Windows	CVE-2021-38629	Windows Ancillary Function Driver for WinSock 信息披露漏洞	Important
Windows	CVE-2021-38630	Windows Event Tracing 权限提升漏洞	Important
Windows	CVE-2021-38632	BitLocker 安全功能绕过漏洞	Important
Windows	CVE-2021-38633	Windows Common Log File System Driver 权限提升漏洞	Important
Windows	CVE-2021-38634	Microsoft Windows Update Client 权限提升漏洞	Important
Windows	CVE-2021-38635	Windows Redirected Drive Buffering SubSystem Driver 信息披露漏洞	Important
Windows	CVE-2021-38636	Windows Redirected Drive	Important

		Buffering SubSystem Driver 信息披露漏洞	
Windows	CVE-2021-38637	Windows Storage 信息披露漏洞	Important
Windows	CVE-2021-38638	Windows Ancillary Function Driver for WinSock 权限提升漏洞	Important
Microsoft Edge (Chromium-based)	CVE-2021-38641	Microsoft Edge for Android 欺骗漏洞	Important
Microsoft Edge (Chromium-based)	CVE-2021-38642	Microsoft Edge for iOS 欺骗漏洞	Important
Azure	CVE-2021-38645	Open Management Infrastructure 权限提升漏洞	Important
Azure	CVE-2021-38648	Open Management Infrastructure 权限提升漏洞	Important
Azure	CVE-2021-38649	Open Management Infrastructure 权限提升漏洞	Important
Microsoft Edge (Chromium-based)	CVE-2021-38669	Microsoft Edge (Chromium-based) 篡改漏洞	Important
Visual Studio Code	CVE-2021-26437	Visual Studio Code 欺骗漏洞	Important
Microsoft Dynamics	CVE-2021-40440	Microsoft Dynamics Business Central 跨站脚本漏洞	Important
Windows	CVE-2021-40444	Microsoft MSHTML 远程代码执行漏洞	Important
Microsoft Edge (Chromium-based)	CVE-2021-36930	Microsoft Edge (Chromium-based) 权限提升漏洞	Important
Azure	CVE-2021-36956	Azure Sphere 信息披露漏洞	Important
Microsoft Visual Studio	CVE-2021-26434	Visual Studio 权限提升漏洞	Important
Windows	CVE-2021-38639	Win32k 权限提升漏洞	Important
Windows	CVE-2021-38644	Microsoft MPEG-2 Video Extension 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38646	Microsoft Office Access Connectivity Engine 远程代码执	Important

		行漏洞	
Microsoft Office	CVE-2021-38650	Microsoft Office 欺骗漏洞	Important
Microsoft Office	CVE-2021-38651	Microsoft SharePoint Server 欺骗漏洞	Important
Microsoft Office	CVE-2021-38652	Microsoft SharePoint Server 欺骗漏洞	Important
Microsoft Office	CVE-2021-38653	Microsoft Office Visio 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38654	Microsoft Office Visio 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38655	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38656	Microsoft Word 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38657	Microsoft Office Graphics Component 信息披露漏洞	Important
Microsoft Office	CVE-2021-38658	Microsoft Office Graphics 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38659	Microsoft Office 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-38660	Microsoft Office Graphics 远程代码执行漏洞	Important
Windows	CVE-2021-38661	HEVC Video Extensions 远程代码执行漏洞	Important
Windows	CVE-2021-38667	Windows Print Spooler 权限提升漏洞	Important
Windows	CVE-2021-38671	Windows Print Spooler 权限提升漏洞	Important
Windows	CVE-2021-40447	Windows Print Spooler 权限提升漏洞	Important
Azure	CVE-2021-40448	Microsoft Accessibility Insights for Android 信息披露漏洞	Important
Microsoft Edge for	CVE-2021-26439	Microsoft Edge for Android 信息	Moderate

Android		披露漏洞	
Microsoft Edge (Chromium-based)	CVE-2021-30606	Chromium: CVE-2021-30606 Use after free in Blink	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30607	Chromium: CVE-2021-30607 Use after free in Permissions	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30608	Chromium: CVE-2021-30608 Use after free in Web Share	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30609	Chromium: CVE-2021-30609 Use after free in Sign-In	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30610	Chromium: CVE-2021-30610 Use after free in Extensions API	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30611	Chromium: CVE-2021-30611 Use after free in WebRTC	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30612	Chromium: CVE-2021-30612 Use after free in WebRTC	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30613	Chromium: CVE-2021-30613 Use after free in Base internals	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30614	Chromium: CVE-2021-30614 Heap buffer overflow in TabStrip	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30615	Chromium: CVE-2021-30615 Cross-origin data leak in Navigation	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30616	Chromium: CVE-2021-30616 Use after free in Media	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30617	Chromium: CVE-2021-30617 Policy bypass in Blink	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30618	Chromium: CVE-2021-30618 Inappropriate implementation in DevTools	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30619	Chromium: CVE-2021-30619 UI Spoofing in Autofill	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30620	Chromium: CVE-2021-30620 Insufficient policy enforcement in	Unknown

		Blink	
Microsoft Edge (Chromium-based)	CVE-2021-30621	Chromium: CVE-2021-30621 UI Spoofing in Autofill	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30622	Chromium: CVE-2021-30622 Use after free in WebApp Installs	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30623	Chromium: CVE-2021-30623 Use after free in Bookmarks	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30624	Chromium: CVE-2021-30624 Use after free in Autofill	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-30632	Chromium: CVE-2021-30632 Out of bounds write in V8	Unknown

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。