Microsoft 发布 2025 年 9 月安全更新

2025-09-10 15:57:51

安全公告编号:CNTA-2025-0012

9 月 10 日，微软发布了 2025 年 9 月的月度例行安全公告，修复了多款产品存在的 86 个安全漏洞,影响产品包括Windows 11、Windows 10、Windows Server 2022、Windows Server 2019 和 Windows Server 2008 等。

利用上述漏洞，攻击者可进行欺骗、绕过安全功能限制、获取敏感信息、提升权限、执行远程代码、或发起拒绝服务攻击等，值得关注的漏洞如下表所示。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2025-54918	Windows NTLM 权限提升漏洞	重要 权限提升	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016 Server 2025 Server 2022 Server 2019 Windows 11 Windows 10
CVE-2025-54910	Microsoft Office 远程代码执行漏洞	重要 远程代码执行	Office 2016 Office LTSC for Mac 2024 Office LTSC 2024 Office LTSC 2021 Office LTSC for Mac 2021 365 Apps for Enterprise Office 2019
CVE-2025-55224	Windows Hyper-V 远程代码执行漏洞	重要 远程代码执行	Server 2025 Server 2022 Server 2019 Windows 10 Windows 11

CVE-2025-55228	Windows Graphics 组件远程代码执行漏洞	重要 远程代码执行	Server 2025 Server 2022 Windows 10 Windows 11
CVE-2025-55226	Graphics Kernel 远程代码执行漏洞	一般 远程代码执行	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016 Server 2025 Server 2022 Server 2019 Windows 10 Windows 11
CVE-2025-55236	Graphics Kernel 远程代码执行漏洞	一般 远程代码执行	Server 2025 Server 2022 Server 2019 Windows 10 Windows 11
CVE-2025-53800	Windows Graphics 组件权限提升漏洞	重要 权限提升	Server 2016 Server 2025 Server 2022 Server 2019 Windows 10 Windows 11
CVE-2025-53804	Windows Kernel-Mode Driver 信息泄露漏洞	中等 信息泄露	Server 2012 R2 Server 2012 Server 2019 Server 2016 Server 2025 Server 2022 Windows 10 Windows 11
CVE-2025-53803	Windows Kernel Memory 信息泄露漏洞	中等 信息泄露	Server 2012 R2 Server 2012 Server 2016 Server 2025 Windows 10 Windows 11
CVE-2025-55234	Windows SMB 权限提升漏洞	严重 权限提升	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016

			Server 2025 Server 2022 Server 2019 Windows 10 Windows 11
CVE-2025-54098	Windows Hyper-V 权限提升漏洞	重要 权限提升	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016 Server 2025 Server 2022 Windows 10 Windows 11
CVE-2025-54916	Windows NTFS 远程代码执行漏洞	重要 远程代码执行	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016 Server 2025 Server 2022 Windows 10 Windows 11
CVE-2025-54093	Windows TCP/IP Driver 权限提升漏洞	重要 权限提升	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016 Server 2025 Server 2022 Windows 10 Windows 11
CVE-2025-54110	Windows Kernel 权限提升漏洞	重要 权限提升	Server 2012 R2 Server 2012 Server 2008 R2 Server 2008 Server 2016 Server 2025 Server 2022 Server 2019 Windows 10 Windows 11

参考信息：

https://msrc.microsoft.com/update-guide/releaseNote/2025-Sep

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

在发布漏洞公告信息之前，CNVD 都力争保证每条公告的准确性和可靠性。然而，采纳和实施公告中的建议则完全由用户自己决定，其可能引起的问题和结果也完全由用户承担。是否采纳我们的建议取决于您个人或您企业的决策，您应考虑其内容是否符合您个人或您企业的安全策略和流程。

我们鼓励所有计算机与网络安全研究机构，包括厂商和科研院所，向我们报告贵单位所发现的漏洞信息。我们将对漏洞信息进行验证，并在 CNVD 网站公布漏洞信息及指导受影响用户采取措施以避免损失。