Microsoft 发布 2025 年 4 月安全更新

2025-04-09 14:18:08

安全公告编号:CNTA-2025-0006

4 月 9 日，微软发布了 2025 年 4 月份的月度例行安全公告，修复了多款产品存在的 126 个安全漏洞,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。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-2025-29824	Windows Common Log File System Driver 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 11 Windows 10
CVE-2025-27480	Windows Remote Desktop Services 远程代码执行漏洞	重要 远程代码执行	Server 2025 Server 2022 Server 2019 Server 2012 R2 Server 2012 Server 2016
CVE-2025-26670	Lightweight Directory Access Protocol (LDAP) Client 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-2025-27482	Windows Remote Desktop Services 远程代码执行漏洞	重要 远程代码执行	Server 2022 Server 2025 Server 2019 Server 2016
CVE-2025-26663	Windows Lightweight Directory Access Protocol (LDAP)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 Server 2019 Windows 10 Windows 11
CVE-2025-27491	Windows Hyper-V 远程代码执行漏洞	重要 远程代码执行	Windows 10 Windows 11 Server 2022 Server 2019 Server 2016 Server 2025
CVE-2025-29791	Microsoft Excel 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 for Mac 2021 Office LTSC 2024 Office LTSC 2021 365 Apps for Enterprise Office 2019
CVE-2025-27752	Microsoft Excel 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-2025-27749	Microsoft Office 远程代码执行漏洞	重要 远程代码执行	Office LTSC 2024 Office LTSC 2021 Office LTSC for Mac 2021 365 Apps for Enterprise Office 2016 Office LTSC for Mac 2024 Office 2019

CVE-2025-27748	Microsoft Office 远程代码执行漏洞	重要 远程代码执行	Office LTSC 2024 Office LTSC 2021 Office LTSC for Mac 2021 365 Apps for Enterprise Office 2016 Office LTSC for Mac 2024 Office 2019
CVE-2025-27745	Microsoft Office 远程代码执行漏洞	重要 远程代码执行	Office LTSC 2024 Office LTSC 2021 Office LTSC for Mac 2021 365 Apps for Enterprise Office 2016 Office LTSC for Mac 2024 Office 2019
CVE-2025-26686	Windows TCP/IP 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 Server 2019 Windows 10 Windows 11
CVE-2025-29812	DirectX Graphics Kernel 权限提升漏洞	重要 权限提升	Server 2025 Server 2022 Windows 11
CVE-2025-27727	Windows Installer 权限提升漏洞	重要 权限提升	Server 2025 Server 2019 Server 2008 R2 Server 2008 Server 2022 Server 2012 R2 Server 2012 Server 2016 Windows 11 Windows 10
CVE-2025-29809	Windows Kerberos 安全功能绕过漏洞	重要 安全功能绕过	Windows 11 Windows 10 Server 2025 Server 2022 Server 2019 Server 2022 Server 2016

CVE-2025-29794	Microsoft SharePoint 远程代码执行漏洞	重要 远程代码执行	SharePoint Server Subscription Edition SharePoint Server 2019 SharePoint Enterprise Server 2016
CVE-2025-29792	Microsoft Office 权限提升漏洞	重要 权限提升	Office 2016 Office LTSC 2024 Office LTSC 2021 365 Apps for Enterprise Office 2019
CVE-2025-29793	Microsoft SharePoint 远程代码执行漏洞	重要 远程代码执行	SharePoint Server Subscription Edition SharePoint Server 2019 SharePoint Enterprise Server 2016
CVE-2025-27472	Windows Mark of the Web 安全功能绕过漏洞	重要 安全功能绕过	Server 2012 R2 Server 2012 Windows 10

参考信息：

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

感谢奇安信网神信息技术（北京）股份有限公司为本报告提供的支持。

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。我们将对所有漏洞信息进行验证并在 CNCERT/CC 网站和国家信息安全漏洞共享平台（CNVD）公布漏洞信息及指导受影响用户采取措施以避免损失。