微软 10 月安全更新多个产品高危漏洞通告

■ **通告编号**	**NS-2022-00**	■ 发布日期	**2022-10-12**
■ **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、Microsoft Office、Hyper-V、Visual Studio Code		

一. 漏洞概述

10 月 12 日，绿盟科技 CERT 监测到微软发布 10 月安全更新补丁，修复了 84 个安全问题，涉及 Windows、Microsoft Office、Visual Studio Code、Hyper-V 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 13 个，重要（Important）漏洞有 71 个，其中包括 2 个 0day 漏洞：

Windows COM+ Event System Service 权限提升漏洞（CVE-2022-41033）

Microsoft Office 信息泄露漏洞（CVE-2022-41043）

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-2022-37979、CVE-2022-38048、CVE-2022-41038、CVE-2022-34689 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 V6.0R02F01.2901，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/vulsys

参考链接：

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

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：

Azure Arc-enabled Kubernetes cluster Connect 权限提升漏洞（CVE-2022-37968）：

Azure Arc-enabled Kubernetes cluster Connect 中存在一个权限提升漏洞，未经身份验证的远程攻击者在了解启用 Azure arc 的 Kubernetes 集群随机生成的外部 DNS 端点后，通过利用此漏洞可实现权限提升，并获得对 Kubernetes 集群的控制。此外，微软官方表示：由于 Azure Stack Edge 允许客户通过 Azure Arc 在其设备上部署 Kubernetes 工作负载，因此 Azure Stack Edge 设备也容易受到此漏洞的攻击，CVSS 评分为 10.0。

官方通告链接：

https://msrc.microsoft.com/update-guide/ch-ZN/vulnerability/CVE-2022-37968

Microsoft Office 远程代码执行漏洞（CVE-2022-38048）：

Microsoft Office 中存在远程代码执行漏洞，攻击者可通过制作恶意的文件，当成功诱导用户在受影响的系统上下载并打开恶意文件后，无需身份验证的本地攻击者可利用该漏洞在目标系统上以用户权限执行任意代码。CVSS 评分为 7.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38048

Microsoft SharePoint Server 远程代码执行漏洞（CVE-2022-41038）：

Microsoft SharePoint 服务器存在远程代码执行漏洞，经过身份验证且具有 ManageList 权限的攻击者通过利用该漏洞，最终可实现在目标服务器上执行任意代码，CVSS 评分为 8.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41038

Windows Hyper-V 权限提升漏洞（CVE-2022-37979）：

Windows Hyper-V 是 Microsoft 的本地虚拟机管理程序。由于 Hyper-V 的安全限制存在缺陷，在特定配置条件下，无需身份验证的本地攻击者通过利用该漏洞可在目标系统上提升至一级 Hyper-V WindowsRootOS 权限。此外，据微软官方表示，成功利用该漏洞可能会对 Hyper-V 主机的功能造成影响。CVSS 评分为 7.8。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37979

Active Directory Certificate Services 权限提升漏洞（CVE-2022-37976）：

Active Directory 证书服务中存在权限提升漏洞，拥有低权限的远程攻击者通过利用该漏洞，可实现在目标系统上提升至域管理员权限，且无需用户交互。且仅当 ActiveDirectory 证书服务在域上运行时，系统受该漏洞影响。CVSS 评分为 9.8。

活动目录（Active Directory）是面向 Windows Standard Server、Windows Enterprie Server 以及 Windows Datacenter Server 的目录服务。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976

Windows CryptoAPI 欺骗漏洞（CVE-2022-34689）：

Windows CryptoAPI 中存在欺骗漏洞，无需身份验证的远程攻击者可通过操纵现有的