医院民航瘫痪-微软服务器-出现重安全漏洞-黑客全球发起攻击

2025年7月18日，全球网络安全界掀起轩然大波。微软SharePoint服务器被曝存在零日漏洞CVE-202
5-53770，黑客利用该漏洞发起大规模攻击，波及美国、欧洲、亚洲等多国机构，医院、民航系统首当其冲，陷入瘫痪
。攻击导致至少75家机构服务器被入侵，敏感数据被窃，引发全球对微软产品安全性的强烈质疑。 事件始于荷兰网络安全
公司Eye Security的发现。7月18日，该公司检测到异常活动，黑客通过SharePoint服务器的To
olPane端点layouts15ToolPaneaspx利用HTTP Referer头漏洞，绕过身份验证，窃
取服务器MachineKey配置，包括ValidationKey和DecryptionKey。

这些密钥让黑客可生成伪造的VIEWSTATE有效载荷，实现远程代码执行。攻击者随后植入后门如spinstall
0aspx，确保即使服务器修补后仍能持续访问。Eye Security扫描全球8000多台SharePoint
服务器，发现至少54家机构已遭入侵，受害者包括银行、医院、大学及政府部门。 独家消息透露，此次攻击由疑似中国背
景的“威胁行动者”主导，谷歌旗下Mandiant确认部分攻击与“中国关系”有关。

攻击目标高度精准，美国教育部、佛罗里达州税务局、罗德岛州议会等机构均被攻破。医院系统尤为严重，攻击导致预约系统
瘫痪，手术被迫取消，患者数据泄露风险激增。民航系统也未能幸免，亚太某航空公司因SharePoint服务器被入侵
，航班调度系统一度中断，造成数千航班延误，旅客滞留机场，混乱不堪。 微软于7月19日发布紧急警报，承认漏洞影响
SharePoint 2016、2019及订阅版服务器，但云端SharePoint Online未受波及。

公司迅速为2019及订阅版发布补丁，但2016版修复仍在开发中，建议用户启用AMSI防病毒接口或断开服务器网络
连接。专家警告，补丁无法完全清除已植入的后门，需额外轮换加密密钥。Palo Alto Networks的Mic
hael Sikorski指出，攻击者已窃取敏感数据、部署持久后门，受害机构需假设系统已被全面攻陷。 社交媒体
上，受害者与网友怒火中烧。某医院员工发帖称：“系统瘫痪，病人资料全丢，手术都停了，微软得负责！

”民航旅客也在X上抱怨：“航班乱套，滞留机场十小时，微软漏洞害惨人！”舆论矛头直指微软，质疑其为何未能提前发现
零日漏洞。此前，微软因Exchange服务器被中国黑客攻击已饱受批评，此次事件进一步动摇了其信誉。 网络安全专
家分析，SharePoint漏洞的高危性在于其无需用户交互即可攻破，且与Outlook、Teams等服务互联，
一旦沦陷，后果不堪设想。美国CISA已将CVE-2025-53770列入已知漏洞目录，要求联邦机构7月21日前
修复。

全球超1万台服务器面临风险，涉及医疗、金融、能源等行业。 目前，FBI、CISA及国际伙伴正联合调查，追查黑客
身份与攻击动机。微软承诺加速修复，并与全球安全机构合作减轻影响。然而，医院与民航的瘫痪已造成巨大损失，公众对科
技巨头的信任再度受挫。这场全球网络攻击的后续影响，将如何重塑企业安全策略?