

存在 DLL 文件被劫持的漏洞报告

尊敬的天翼云用户：
您好！

安全测试发现，SSL VPN 设备 7.5 版本存在 DLL 文件被劫持的漏洞，该漏洞存在于 SSL VPN7.5 版本的产品中，攻击者将 EasyConnect 客户端安装包以及伪造的 DLL 文件一同发至客户处并诱导客户点击执行，基于 Windows 特性系统会调用当前目录的伪造 DLL 文件，可能造成恶意指令被执行。

经过分析与确认，受影响的产品范围为 SSL VPN7.5 的版本。存量用户可能存在未修复的情况。可通过更新最新版本的安全修复补丁即可修复该漏洞问题。开启“允许自动更新”功能的客户已完成了在线自动修复。

【影响版本】

SSL VPN 7.5 版本

【安全版本】

SSLVPN7.6.8R2 版本

【修复方案】

更新 SP_SSL_IMPROVE_COM(20230620) 补丁包可解决以上问题，开启“允许自动更新”功能的客户已完成了在线自动修复。补丁包需提工单获取

【产品使用安全建议】

1. 定期进行管理员密码修改，且满足一定的密码复杂度。建议包含大写、小写、特殊字符、数字至少三种的组合方式；
2. 设置当前产品的控制台登录 IP 地址白名单限制，只允许运维人员的 IP 地址登录控制台；
3. 关闭当前产品非必要开放端口，如远程维护端口、SSH 端口。

如需帮助请通过在线工单或 400 热线联系我们，我们将第一时间提供响应和支持。

天翼云服务团队
2020 年 11 月 3 日