

安全访问设备状态间歇性"；过期" 错误

目录

问题

Cisco Secure Access中的Device Posture间歇性地显示已注册设备的“过期”状态，从而阻止零信任访问状态验证。

用户在特定时间段内会遇到以下错误消息：

- “您的设备状态已过期”
- “无法自动运行设备的安全检查”

尽管Duo Desktop表示完全遵守所有安全要求（包括Windows更新、系统密码配置、BitLocker加密和防火墙启用），但仍会发生此问题。在出现问题的期间，尝试注销并重新注册受影响的设备会因内部错误而失败。恢复正常操作的唯一临时解决方法是执行完整的系统重启，这会中断用户访问和工作效率。

其他症状包括：AnyConnect VPN在整个问题期间保持连接，而零信任访问注册和安全状态验证流程在可预测的时间段内间歇性失败。

环境

- 启用设备状态功能的思科安全访问
- 用于设备合规性验证的双桌面客户端
- 启用BitLocker加密、系统密码和Windows防火墙的Windows终端
- 需要状态验证的零信任访问部署
- 在思科安全访问中配置的状态配置文件匹配设备合规性状态

分辨率

通过将Cisco安全访问客户端升级到最新版本5.1.15.287解决了此问题。此版本解决了导致间歇性设备状态验证失败的基本缺陷。

客户端升级过程

步骤 1：确定受影响终端上的当前客户端版本。

通过应用界面或系统安装记录验证现有的Cisco Secure Access客户端版本。

步骤 2：下载并部署客户端版本5.1.15.287。

从相应的思科分发渠道获取更新的客户端软件，并部署到遇到设备状态验证问题的所有受影响终端。

步骤 3：检验分辨率。

完成客户端升级后，监控之前有问题的时间段内的设备状态以确认稳定运行，无需系统重新启动。



注意：建议安装最新版本的Secure Client。

验证步骤

客户端升级后，请验证：

- 设备状态验证在之前有问题的时间段内成功完成。
- 无信任访问注册功能，无内部错误。
- 根据需要成功完成取消注册和重新注册操作。
- 无需重新启动系统即可保持设备状态合规性。

- Duo Desktop和Cisco Secure Access状态保持同步。

原因

间歇性设备状态验证失败是由Cisco Bug ID CSCws68569引起的。此缺陷影响了Cisco Secure Access客户端与状态验证服务之间的通信，导致临时同步问题，从而阻止在特定操作窗口期间准确报告设备合规性状态。

相关内容

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。