Firefox和Safari在macOS上的安全访问自定义CA信任问题

目录

问题

用户在macOS浏览器（Safari和Firefox）中通过Cisco安全访问访问已解密的互联网流量时遇到证书信任错误。Chrome浏览器工作正常，但Safari和Firefox显示“不可信证书”警告，并阻止访问网站和应用。

完整的证书链显示：

- 网站（例如cnn.com）> Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Firefox和Safari浏览器在思科中间证书处停止了证书验证，并且无法链至根CA，而Chrome已成功验证整个证书链。

环境

- 具有用于HTTPS解密的自定义证书颁发机构的思科安全访问部署
- 带Safari和Firefox浏览器的macOS设备
- 使用Microsoft证书颁发机构的自定义CA证书基础设施
- 启用解密和入侵防御的互联网访问策略
- 组织ID:xxxxx

分辨率

通过识别证书链中的编码不匹配并切换到思科安全访问根CA进行解密，解决了此问题。

根本原因分析

团队发现自定义证书颁发机构是使用可打印的字符串编码创建的，即使叶证书设置为UTF8STRING，也会导致不兼容问题。Firefox和Safari要求链中的所有证书的格式相同，而Chrome没有此严格要求。

解决步骤

切换到Cisco安全访问根CA

替代解决方案

如果需要使用自定义CA，则确定以下选项：

- 使用UTF8编码重建整个证书基础设施（建议不要使用高影响）
- 使用支持UTF8编码的不同证书基础设施
- Firefox和Safari的限制无法与当前自定义CA设置配合使用

原因

根本原因是Microsoft证书颁发机构（默认情况下使用printablestring编码）和Cisco安全访问使用的UTF8链之间的编码不匹配。Firefox和Safari具有更严格的证书验证要求，并且需要链中的所有证书才能使用一致的编码。Chrome中更宽松的验证允许它使用混合编码链，而Firefox和Safari则拒绝不一致的证书格式。

Microsoft CA使用printablestring编码创建证书，但Cisco Secure Access中间证书使用UTF8STRING编码。这种不匹配导致Firefox和Safari无法在Cisco中间证书级别验证证书链。

相关内容

- 在SWG中配置Webex会议访问
- 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）。