MacOS上Firefox和Safari的安全訪問自定義CA信任問題

目錄

問題

使用者在通過Cisco Secure Access訪問已解密的網際網路流量時，在macOS瀏覽器（Safari和Firefox）中遇到證書信任錯誤。Chrome瀏覽器工作正常，但Safari和Firefox顯示「不可信證書」警告，並阻止訪問網站和應用。

完整的證書鏈顯示：

- 網站(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瀏覽器已停止在思科中間證書上的證書驗證，並且無法鏈結到根CA，而Chrome已成功驗證整個證書鏈。

環境

- 具有用於HTTPS解密的自定義證書頒發機構的思科安全訪問部署
- 使用Safari和Firefox瀏覽器的MacOS裝置
- 使用Microsoft證書頒發機構自定義CA證書基礎架構
- 啟用解密和入侵防禦的Internet訪問策略
- 組織ID:xxxxx

解析

通過識別憑證鏈中的編碼不相符並切換至思科安全存取根CA進行解密，問題得以解決。

根本原因分析

團隊發現自定義證書頒發機構是使用可列印的字串編碼建立的，即使葉證書設定為UTF8STRING，也會導致不相容問題。Firefox和Safari要求鏈中的所有證書格式相同，而Chrome則沒有這種嚴格的要求。

解決步驟

切換到思科安全訪問根CA

替代解決方案

如果需要使用自訂CA，則會識別以下選項：

- 使用UTF8編碼重建整個證書基礎架構（建議不要採用高影響）
- 使用支援UTF8編碼的不同證書基礎架構
- Firefox和Safari的限制無法與當前自定義CA設定配合使用

原因

根本原因是Microsoft證書頒發機構（預設情況下使用printablestring編碼）和Cisco Secure Access使用的UTF8鏈之間的編碼不匹配。Firefox和Safari具有更嚴格的證書驗證要求，需要使用鏈中的所有證書才能使用一致的編碼。Chrome中更寬鬆的驗證允許它使用混合編碼鏈，而Firefox和Safari則拒絕不一致的證書格式。

Microsoft CA使用printablestring編碼建立證書，但Cisco Secure Access中間證書使用UTF8STRING編碼。這種不匹配導致Firefox和Safari無法在Cisco中間證書級別驗證證書鏈。

相關內容

- 在SWG中配置Webex會議訪問
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。