Splunk客戶端日誌上載時出現安全訪問證書驗證錯誤

目錄

問題

由於證書驗證錯誤，運行Splunk客戶端的Windows客戶端無法向Splunk雲上傳日誌，當時流量被Cisco Secure Access解密。超過5000個Windows日誌源無法將資料傳送到Splunk雲，影響日誌接收。在Splunk客戶端日誌中觀察到的特定錯誤為：

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

到達目標*.splunkcloud.com的流量通過防火牆流動，但應用級證書驗證失敗。瀏覽到啟用SSL解密的網站的操作繼續正常運行。

環境

- 啟用SSL/TLS解密的Cisco安全訪問
- 安裝了Splunk Universal Forwarder的Windows客戶端
- Splunk雲目標：*.splunkcloud.com
- 受影響的日誌源超過5000個
- Splunk客戶端使用其自己的證書儲存，而不是Microsoft系統證書儲存

解析

通過在思科安全訪問中為Splunk雲流量實施解密繞過策略解決了此問題。

已採取了若干步驟。

步驟 1:找出問題

在WebEx會議期間，該行為被確認並再次出現。測試表明，當客戶端禁用安全訪問解密或客戶端上禁用SWG服務時，Splunk日誌上傳成功。這確認了SSL/TLS解密過程導致證書驗證失敗。

步驟 2:建立目標清單

已建立包含Splunk雲FQDN和IP地址的目的地清單，該清單特別針對目的地為Splunk雲服務的流量。

步驟 3:實施解密旁路策略

已實施思科安全訪問策略以禁用與Splunk雲目標清單匹配的流量的SSL/TLS解密。此繞過策略允許Splunk客戶端建立到Splunk雲的直接加密連線，而無需安全訪問進行證書攔截。

步驟 4:驗證

實施解密旁路策略後，驗證確認：

- Splunk客戶端能夠成功上傳日誌
- Splunk雲中報告客戶端的總數顯著增加
- 未觀察到其他證書驗證錯誤

案例嚴重性從1降低到3，並置於監控狀態以觀察持續的成功日誌攝取。

原因

根本原因是Splunk客戶端使用其自己的證書儲存區，並且不信任在SSL/TLS解密過程中呈現的Cisco Secure Access Primary SubCA證書。當思科安全訪問截獲並解密到Splunk雲的SSL流量時，它會使用自己的證書頒發機構重新加密流量。Splunk客戶端證書驗證進程拒絕此證書，因為它無法驗證證書鏈返回至其自身證書儲存中的受信任的根證書頒發機構。

特定的X.509驗證錯誤「無法獲取本地頒發者證書」（錯誤代碼20）表示證書驗證進程無法在客戶端受信任證書儲存中找到頒發證書頒發機構，從而導致連線失敗。

相關內容

- 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）。