# Telepresence SUDI證書鏈安全掃描查詢結果故障排除

## 目錄

## 問題

安全漏洞掃描正在標籤Cisco Telepresence影片編解碼器終端上的SSL/TLS證書相關發現，特別是報告TCP埠4053、4060和4062上的不受信任證書鏈。漏洞掃描程式可識別編解碼器，它提供由ACT2 SUDI CA(組織：Cisco)，證書鏈終止於思科根CA 2048。安全掃描系統將此報告為不滿足組織安全要求的不可信證書鏈。

安全掃描報告的特定查詢結果包括：

- 自簽名證書檢測
- 不受信任的證書鏈
- 弱雜湊演算法問題
- 證書到期警告

## 環境

- Cisco Telepresence視訊編解碼器終端
- 具有內部部署註冊的Webex案頭系列裝置
- 採用ACT2 SUDI（安全唯一裝置識別符號）晶片的終端
- 標籤證書鏈問題的安全漏洞掃描基礎設施
- 顯示SUDI證書的TCP埠4053、4060和4062

# 解析

Cisco Telepresence端點上的SUDI憑證是內嵌的、不可變的憑證，不能以支援的方式加以修改、重新產生或刪除。這些證書是思科Trustworthy Technologies實施的一部分，用於特定安全功能。

## 瞭解SUDI證書行為

憑證行為因連線埠和系統組態而異：

- 埠4053（配對服務）：當系統具有ACT2晶片時，使用SUDI證書。自定義證書僅在沒有ACT2晶片（舊端點）的系統上使用。
- Port 4047:使用客戶選擇的證書在觸控面板和編解碼器之間進行通訊。

## 證書位置和詳細資訊

SUDI證書位於裝置的證書儲存區中：

```
device:~] $ cd /etc/cacerts_sudi
device:/etc/cacerts_sudi] $ ls
0763c37d.0                9426d327.0                mic-cbasrcarsa4k2099.pem
29cf4e89.0                a094437b.0                mic-cmca.pem
36087b08.0                b35c8d6c.0                mic-cmca2.pem
417aa245.0                cmca2.pem                 mic-cmca3.pem
771a09b9.0                crca2048.pem              mic-cmca4.pem
89087fe6.0                crca2099.pem              mic-crcam2.pem
90359431.0                mic-cbarc2099.pem         mic-harsa-ca.pem
```

ACT2 SUDI CA證書詳細資訊：

```
CN = ACT2 SUDI CA
O = Cisco
Valid From: Thursday, June 30, 2011 11:26:57 PM
Valid To: Tuesday, May 15, 2029 1:55:42 AM
```

## 建議的操作

步驟 1:審查SUDI證書用途和安全實施

SUDI證書不是自簽名的，而是由Cisco Manufacturing CA簽名的。它充當不可變的身份憑證，能夠：

- 維護產品識別符號和序列號
- 為配置、安全、審計和管理提供不可更改的標識
- 以密碼方式繫結到信任錨點模組晶片
- 使克隆或欺騙變得幾乎不可能

步驟 2:與安全團隊合作排除SUDI證書查詢結果

由於SUDI證書無法修改，且無法提供合法的安全功能，因此建議採用以下方法：

- 配置安全掃描工具以排除受影響服務的SUDI證書鏈查詢結果
- 根據思科的Trustworthy Technologies實施記錄例外情況的業務理由
- 如果需要，將安全掃描重點放在其他埠上的客戶可配置證書上

步驟 3:通過軟體升級進行證書更新

當系統升級到較新的軟體版本時，信任儲存中的證書更新會自動發生。這可確保隨時間推移保持憑證有效性。

## 重要限制

以下限制適用於SUDI證書：

- 無法修改、重新生成或刪除
- 如果刪除證書並重新啟動裝置，則會自動重新生成
- 不存在將可配置證書分配給這些後端服務的受支援方法

- 由於信任錨點實現不可變的性質，無法替換證書

## 原因

安全掃描發現由思科的SUDI（安全唯一裝置識別符號）證書觸發，這些證書是連結到思科根CA 2048的嵌入式製造證書。這些證書是思科Trustworthy Technologies實施的一部分，出於安全目的設計為不可變。組織安全掃描工具不會將證書識別為受信任，因為它們終止於思科的根證書頒發機構，而不是組織特定的CA。這是啟用SUDI的裝置的預期行為，代表設計功能而非安全漏洞。

## 相關內容

- Cisco Trustworthy Technologies資料表
- 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）。