Fehlerbehebung: Telepresence SUDI Certificate Chain Sicherheits-Suchergebnisse

Inhalt

Problem

Scans auf Sicherheitslücken zeigen SSL/TLS-zertifizierungsrelevante Ergebnisse auf Cisco TelePresence-Video-Codec-Endgeräten an. Es wird eine nicht vertrauenswürdige Zertifikatkette auf den TCP-Ports 4053, 4060 und 4062 gemeldet. Der Scanner identifiziert den Codec und stellt ein CS-Room-Zertifikat dar, das von der ACT2 SUDI CA (Organisation: Cisco), wobei die Zertifikatskette bei der Cisco Root CA 2048 endet. Das Sicherheits-Scanning-System meldet dies als nicht vertrauenswürdige Zertifikatkette, die die Sicherheitsanforderungen der Organisation nicht erfüllt.

Die Sicherheitsscans lieferten folgende Ergebnisse:

- Selbstsignierte Zertifikaterkennung
- Nicht vertrauenswürdige Zertifikatkette
- Schwachstellen bei Hash-Algorithmen
- Warnung vor Ablauf des Zertifikats

Umwelt

- Cisco TelePresence Video-Codec-Endgeräte
- Geräte der WebEx Desk-Serie mit standortbasierter Registrierung
- Endgeräte mit ACT2 SUDI-Chips (Secure Unique Device Identifier)
- Infrastruktur für das Scannen von Sicherheitslücken kennzeichnet Probleme mit der Zertifikatkette

- Die TCP-Ports 4053, 4060 und 4062 stellen SUDI-Zertifikate dar.

Auflösung

Die SUDI-Zertifikate auf Cisco TelePresence-Endpunkten sind eingebettete, unveränderliche Zertifikate, die nicht auf unterstützte Weise geändert, regeneriert oder gelöscht werden können. Diese Zertifikate sind Teil der Cisco Trustworthy Technologies-Implementierung und dienen spezifischen Sicherheitsfunktionen.

Das Verhalten von SUDI-Zertifikaten

Das Zertifikatverhalten variiert je nach Port- und Systemkonfiguration:

- Port 4053 (Kopplungsdienst): Verwendet SUDI-Zertifikate, wenn das System über einen ACT2-Chip verfügt. Benutzerdefinierte Zertifikate werden nur auf Systemen ohne ACT2-Chip (ältere Endgeräte) verwendet.
- Port 4047: Verwendet vom Kunden ausgewählte Zertifikate für die Kommunikation zwischen Touchpanels und Codecs.

Zertifikatspeicherort und -details

Die SUDI-Zertifikate befinden sich im Zertifikatspeicher des Geräts:

```
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
```

Details zum ACT2 SUDI CA-Zertifikat:

```
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
```

Empfohlene Maßnahmen

Schritt 1: Prüfung von Zweck und Sicherheitsimplementierung des SUDI-Zertifikats

Das SUDI-Zertifikat ist nicht selbstsigniert, sondern wird von der Cisco Manufacturing CA signiert. Es dient als unabänderlicher Identitätsnachweis, der:

- Behält Produkt-ID und Seriennummer bei
- Bietet eine unveränderliche Identität für Konfiguration, Sicherheit, Audit und Management
- kryptografisch an den Trust Anchor-Modulchip gebunden ist
- Klonen oder Spoofing praktisch unmöglich

Phase 2: Ausschließen der Ergebnisse von SUDI-Zertifikaten in Zusammenarbeit mit dem Sicherheitsteam

Da die SUDI-Zertifikate nicht geändert werden können und legitime Sicherheitsfunktionen erfüllen, wird folgende Vorgehensweise empfohlen:

- Sicherheitsscantools konfigurieren, um die Ergebnisse der SUDI-Zertifikatkette für die betroffenen Services auszuschließen
- Dokumentieren der geschäftlichen Begründung der Ausnahme basierend auf der Implementierung von Cisco Trustworthy Technologies
- Konzentrieren Sie sich bei Bedarf auf das Scannen von Sicherheitszertifikaten, die vom Kunden konfiguriert werden können.

Schritt 3: Zertifikats-Updates durch Software-Upgrades

Zertifikats-Updates im Vertrauensspeicher werden automatisch durchgeführt, wenn das System auf neuere Softwareversionen aktualisiert wird. So wird sichergestellt, dass die Gültigkeit des Zertifikats über einen längeren Zeitraum erhalten bleibt.

Wichtige Einschränkungen

Diese Einschränkungen gelten für SUDI-Zertifikate:

- Kann nicht geändert, neu generiert oder gelöscht werden
- Die automatische Regeneration erfolgt, wenn Zertifikate gelöscht werden und das Gerät neu startet.
- Es ist keine unterstützte Methode zum Zuweisen konfigurierbarer Zertifikate zu diesen Backend-Services vorhanden.
- Der Austausch von Zertifikaten ist aufgrund des unveränderlichen Charakters der Trust Anchor-Implementierung nicht möglich.

Ursache

Die Ergebnisse der Sicherheitsprüfung werden durch das Vorhandensein von Cisco SUDI-Zertifikaten (Secure Unique Device Identifier) ausgelöst. Dabei handelt es sich um eingebettete Fertigungszertifikate, die an die Cisco Root CA 2048 ketten. Diese Zertifikate sind Teil der Cisco Trustworthy Technologies-Implementierung und aus Sicherheitsgründen unveränderlich. Die Zertifikate werden von organisatorischen Sicherheits-Scanning-Tools nicht als vertrauenswürdig anerkannt, da sie bei der Stammzertifizierungsstelle von Cisco enden und nicht bei einer organisationsspezifischen Zertifizierungsstelle. Dies ist ein erwartetes Verhalten für SUDI-fähige Geräte und stellt eher eine Designfunktion als eine Sicherheitslücke dar.

Verwandte Inhalte

- Datenblatt zu vertrauenswürdigen Technologien von Cisco
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.