Dépannage des résultats du scan de sécurité de la chaîne de certificats SUDI TelePresence

Table des matières

Problème

Les analyses des vulnérabilités de sécurité signalent les découvertes liées aux certificats SSL/TLS sur les terminaux de codecs vidéo Cisco Telepresence, en signalant spécifiquement une chaîne de certificats non fiables sur les ports TCP 4053, 4060 et 4062. L'analyseur de vulnérabilité identifie le codec et présente un certificat CS-Room délivré par l'AC ACT2 SUDI (Organisation : Cisco), la chaîne de certificats se terminant au niveau de Cisco Root CA 2048. Le système d'analyse de sécurité signale ceci comme une chaîne de certificats non approuvée qui ne répond pas aux exigences de sécurité de l'organisation.

Les résultats spécifiques signalés par les analyses de sécurité incluent :

- Détection de certificat auto-signé
- Chaîne de certificats non approuvée
- Problèmes d'algorithme de hachage faible
- Avertissements d'expiration de certificat

Environnement

- Terminaux de codec vidéo Cisco TelePresence
- Périphériques de la gamme Webex Desk avec enregistrement sur site
- Terminaux avec puces ACT2 SUDI (Secure Unique Device Identifier)
- Infrastructure d'analyse des vulnérabilités de sécurité signalant les problèmes de chaîne de certificats

- Ports TCP 4053, 4060 et 4062 présentant des certificats SUDI

Résolution

Les certificats SUDI sur les terminaux Cisco Telepresence sont des certificats immuables intégrés qui ne peuvent pas être modifiés, régénérés ou supprimés de manière prise en charge. Ces certificats font partie de la mise en oeuvre de Cisco Trustworthy Technologies et remplissent des fonctions de sécurité spécifiques.

Présentation du comportement des certificats SUDI

Le comportement du certificat varie selon le port et la configuration du système :

- Port 4053 (service de jumelage) : Utilise des certificats SUDI lorsque le système dispose d'une puce ACT2. Les certificats personnalisés ne sont utilisés que sur les systèmes sans puce ACT2 (terminaux plus anciens).
- Port 4047 : Utilise les certificats choisis par le client pour la communication entre les écrans tactiles et les codecs.

Emplacement et détails du certificat

Les certificats SUDI se trouvent dans le magasin de certificats du périphérique :

```
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
```

Détails du certificat AC ACT2 SUDI :

```
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
```

Actions recommandées

Étape 1: Examiner le rôle du certificat SUDI et la mise en oeuvre de la sécurité

Le certificat SUDI n'est pas auto-signé, mais il est signé par l'autorité de certification Cisco Manufacturing. Il sert de justificatif d'identité immuable qui :

- Conserve l'identifiant et le numéro de série du produit
- Fournit une identité inaltérable pour la configuration, la sécurité, l'audit et la gestion
- Est cryptographiquement lié à la puce du module Trust Anchor
- Rend pratiquement impossible le clonage ou l'usurpation

Étape 2: Collaborer avec l'équipe de sécurité pour exclure les résultats de certificat SUDI

Étant donné que les certificats SUDI ne peuvent pas être modifiés et remplissent des fonctions de sécurité légitimes, l'approche recommandée consiste à :

- Configurez les outils d'analyse de sécurité pour exclure les résultats de la chaîne de certificats SUDI pour les services concernés
- Documenter la justification commerciale de l'exception basée sur la mise en oeuvre des technologies fiables de Cisco
- Concentrer l'analyse de sécurité sur les certificats configurables par le client sur d'autres ports si nécessaire

Étape 3: Mises à jour de certificats via des mises à niveau logicielles

Les mises à jour de certificats dans le magasin de certificats de confiance se produisent automatiquement lorsque le système est mis à niveau vers des versions logicielles plus récentes. Cela garantit que la validité du certificat est conservée au fil du temps.

Limites importantes

Ces limitations s'appliquent aux certificats SUDI :

- Ne peut pas être modifié, régénéré ou supprimé
- La régénération automatique se produit si les certificats sont supprimés et si le périphérique redémarre
- Il n'existe aucune méthode prise en charge pour attribuer des certificats configurables à ces services principaux
- Le remplacement du certificat n'est pas possible en raison de la nature immuable de la mise en oeuvre de Trust Anchor

Motif

Les résultats de l'analyse de sécurité sont déclenchés par la présence des certificats SUDI (Secure Unique Device Identifier) de Cisco, qui sont des certificats de fabrication intégrés qui enchaînent à Cisco Root CA 2048. Ces certificats font partie de la mise en oeuvre des technologies fiables de Cisco et sont conçus pour être immuables à des fins de sécurité. Les certificats ne sont pas reconnus comme fiables par les outils d'analyse de sécurité de l'organisation, car ils se terminent au niveau de l'autorité de certification racine de Cisco plutôt qu'au niveau d'une autorité de certification spécifique à l'organisation. Ce comportement est normal pour les périphériques compatibles SUDI et représente une fonctionnalité de conception plutôt qu'une vulnérabilité de sécurité.

Autres informations utiles

- Fiche technique sur Cisco Trustworthy Technologies
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.