Problemen oplossen met bevindingen van de beveiligingsscan van de SUDI-certificaatketen

Inhoud

uitgifte

Beveiligingsbeveiligingsscans markeren SSL / TLS-certificaatgerelateerde bevindingen op Cisco Telepresence-videocodec-eindpunten, waarbij specifiek een niet-vertrouwde certificaatketen op TCP-poorten 4053, 4060 en 4062 wordt gerapporteerd. De kwetsbaarheidscanner identificeert de codec en presenteert een CS-Room-certificaat dat is uitgegeven door ACT2 SUDI CA (Organisatie: Cisco), waarbij de certificaatketen eindigt op Cisco Root CA 2048. Het beveiligingsscansysteem rapporteert dit als een niet-vertrouwde certificaatketen die niet voldoet aan de beveiligingsvereisten van de organisatie.

De specifieke bevindingen die door beveiligingsscans worden gerapporteerd, zijn onder meer:

- Zelfondertekende certificaatdetectie
- Niet-vertrouwde certificaatketen
- Zwakke hashing algoritme zorgen
- Waarschuwingen voor het vervallen van certificaten

milieu

- Cisco Telepresence video codec eindpunten
- Webex Desk Series-apparaten met on-premises registratie
- Eindpunten met ACT2 SUDI-chips (Secure Unique Device Identifier)
- Problemen met de certificaatketen bij het scannen van beveiligingslekken van infrastructuur
- TCP-poorten 4053, 4060 en 4062 met SUDI-certificaten

resolutie

De SUDI-certificaten op Cisco Telepresence-eindpunten zijn ingesloten, onveranderlijke certificaten die niet kunnen worden gewijzigd, geregenereerd of verwijderd op een ondersteunde manier. Deze certificaten maken deel uit van de Trustworthy Technologies-implementatie van Cisco en dienen specifieke beveiligingsfuncties.

Inzicht in SUDI-certificaatgedrag

Het certificaatgedrag verschilt per poort en systeemconfiguratie:

- Poort 4053 (Pairing Service): gebruikt SUDI-certificaten wanneer het systeem een ACT2-chip heeft. Aangepaste certificaten worden alleen gebruikt op systemen zonder ACT2-chip (oudere eindpunten).
- Poort 4047: gebruikt door de klant gekozen certificaten voor communicatie tussen aanraakpanelen en codecs.

Locatie en details certificaat

De SUDI-certificaten bevinden zich in het certificaatarchief van het apparaat:

```
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
```

Het ACT2 SUDI CA-certificaat vermeldt:

```
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

Aanbevolen acties

Stap 1: Beoordeel het doel van het SUDI-certificaat en de implementatie van de beveiliging

Het SUDI-certificaat is niet zelfondertekend, maar is ondertekend door Cisco Manufacturing CA. Het dient als een onveranderlijk identiteitsbewijs dat:

- Onderhoudt product-id en serienummer
- Biedt een onveranderlijke identiteit voor configuratie, beveiliging, controle en beheer
- Is cryptografisch gebonden aan de Trust Anchor module chip
- Maakt klonen of spoofing vrijwel onmogelijk

Stap 2: Werk samen met het beveiligingsteam om bevindingen van SUDI-certificaten uit te sluiten

Aangezien de SUDI-certificaten niet kunnen worden gewijzigd en legitieme beveiligingsfuncties dienen, is de aanbevolen aanpak:

- Beveiligingsscanningstools configureren om de bevindingen van de SUDI-certificaatketen voor de betrokken services uit te sluiten
- Documenteer de zakelijke rechtvaardiging voor de uitzondering op basis van de Trustworthy Technologies-implementatie van Cisco
- Richt beveiligingsscans indien nodig op door de klant configureerbare certificaten op andere poorten

Stap 3: Certificaatupdates via software-upgrades

Certificaatupdates in de vertrouwenswinkel worden automatisch uitgevoerd wanneer het systeem wordt geüpgraded naar nieuwere softwareversies. Dit zorgt ervoor dat de geldigheid van het certificaat in de loop van de tijd behouden blijft.

Belangrijke beperkingen

Deze beperkingen gelden voor SUDI-certificaten:

- Kan niet worden gewijzigd, geregenereerd of verwijderd
- Automatische regeneratie vindt plaats als certificaten worden verwijderd en het apparaat opnieuw wordt opgestart
- Er bestaat geen ondersteunde methode om configureerbare certificaten toe te wijzen aan deze backendservices
- Certificaatvervanging is niet mogelijk vanwege de onveranderlijke aard van de implementatie van het vertrouwensanker

Oorzaak

De bevindingen van de beveiligingsscan worden geactiveerd door de aanwezigheid van Cisco's SUDI (Secure Unique Device Identifier) -certificaten, die zijn ingesloten productiecertificaten die zijn gekoppeld aan Cisco Root CA 2048. Deze certificaten maken deel uit van de Trustworthy Technologies-implementatie van Cisco en zijn ontworpen om onveranderlijk te zijn voor beveiligingsdoeleinden. De certificaten worden niet herkend als vertrouwd door organisatorische beveiligingsscanningstools omdat ze eindigen bij de root-certificaatautoriteit van Cisco in plaats van een organisatiespecifieke CA. Dit is het verwachte gedrag voor SUDI-apparaten en vertegenwoordigt een ontwerpfunctie in plaats van een beveiligingslek.

Gerelateerde inhoud

- Cisco Trustworthy Technologies-gegevensblad
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.