Solucionar problemas de hallazgos de Telepresence SUDI Certificate Chain Security Scan

Contenido

Problema

Los análisis de vulnerabilidades de seguridad están señalando las conclusiones relacionadas con los certificados SSL/TLS en los terminales de códecs de vídeo de Cisco Telepresence, en concreto, informando sobre una cadena de certificados no fiable en los puertos TCP 4053, 4060 y 4062. El analizador de vulnerabilidades identifica el códec y presenta un certificado de CS-Room emitido por ACT2 SUDI CA (Organization: Cisco) con la cadena de certificados que termina en la CA raíz de Cisco 2048. El sistema de análisis de seguridad informa de que se trata de una cadena de certificados no fiable que no cumple los requisitos de seguridad de la organización.

Las conclusiones específicas de los análisis de seguridad incluyen:

- Detección de certificados autofirmados
- Cadena de certificados no fiable
- Problemas con algoritmos de hash débiles
- Advertencias de vencimiento del certificado

Entorno

- Terminales con códec de vídeo de Cisco Telepresence
- Dispositivos de la serie Webex Desk con registro en las instalaciones
- Terminales con chips ACT2 SUDI (Secure Unique Device Identifier)
- Vulnerabilidad de seguridad al analizar la infraestructura marcando problemas de la cadena

de certificados

- Puertos TCP 4053, 4060 y 4062 que presentan certificados SUDI

Resolución

Los certificados SUDI en los terminales de Cisco Telepresence son certificados integrados e inmutables que no se pueden modificar, regenerar ni eliminar de una manera compatible. Estos certificados forman parte de la implementación de Cisco Trustworthy Technologies y cumplen funciones de seguridad específicas.

Comprensión del Comportamiento del Certificado SUDI

El comportamiento del certificado varía según el puerto y la configuración del sistema:

- Puerto 4053 (servicio de emparejamiento): Utiliza certificados SUDI cuando el sistema tiene un chip ACT2. Los certificados personalizados sólo se utilizan en sistemas sin un chip ACT2 (terminales más antiguos).
- Port 4047: Utiliza certificados elegidos por el cliente para la comunicación entre paneles táctiles y códecs.

Ubicación y detalles del certificado

Los certificados SUDI se encuentran en el almacén de certificados del dispositivo:

```
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
```

Los detalles del certificado de CA SUDI ACT2:

```
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
```

Acciones recomendadas

Paso 1: Revisar el propósito del certificado SUDI y la implementación de seguridad

El certificado SUDI no tiene firma propia, pero está firmado por la CA de Cisco Manufacturing. Sirve como credencial de identidad inmutable que:

- Mantiene el identificador del producto y el número de serie
- Proporciona una identidad inalterable para la configuración, seguridad, auditoría y gestión
- Está enlazado criptográficamente al chip del módulo Trust Anchor
- Hace que la clonación o la suplantación sean prácticamente imposibles

Paso 2: Trabajar con el equipo de seguridad para excluir las conclusiones de los certificados SUDI

Dado que los certificados SUDI no se pueden modificar y cumplen funciones de seguridad legítimas, el enfoque recomendado es:

- Configure las herramientas de análisis de seguridad para excluir las conclusiones de la cadena de certificados SUDI para los servicios afectados
- Documentar la justificación empresarial de la excepción en función de la implementación de tecnologías fiables de Cisco
- Centrar el análisis de seguridad en los certificados configurables por el cliente en otros puertos si es necesario

Paso 3: Actualizaciones de certificados mediante actualizaciones de software

Las actualizaciones de certificados en el almacén de confianza se producen automáticamente cuando el sistema se actualiza a versiones de software más recientes. Esto garantiza que la validez del certificado se mantenga a lo largo del tiempo.

Limitaciones importantes

Estas limitaciones se aplican a los certificados SUDI:

- No se puede modificar, regenerar ni eliminar
- La regeneración automática se produce si se eliminan los certificados y se reinicia el dispositivo
- No existe ningún método admitido para asignar certificados configurables a estos servicios backend
- La sustitución de certificados no es posible debido a la naturaleza inmutable de la implementación de Trust Anchor

Causa

Las conclusiones del análisis de seguridad se activan por la presencia de los certificados SUDI (identificador único de dispositivo seguro) de Cisco, que son certificados de fabricación integrados que se encadenan a la CA raíz de Cisco 2048. Estos certificados forman parte de la implementación de Cisco Trustworthy Technologies y están diseñados para ser inmutables por motivos de seguridad. Las herramientas de análisis de seguridad organizativa no reconocen que los certificados son de confianza porque terminan en la entidad emisora de certificados raíz de Cisco en lugar de en una CA específica de la organización. Este es el comportamiento esperado para los dispositivos con SUDI y representa una función de diseño en lugar de una vulnerabilidad de seguridad.

Contenido relacionado

- Ficha técnica de Cisco Trustworthy Technologies
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).