Solucionar problemas de verificação de segurança da cadeia de certificados SUDI do Telepresence

Contents

Problema

As varreduras de vulnerabilidade de segurança estão sinalizando descobertas relacionadas ao certificado SSL/TLS em endpoints de codec de vídeo Cisco Telepresence, relatando especificamente uma cadeia de certificados não confiáveis nas portas TCP 4053, 4060 e 4062. O verificador de vulnerabilidade identifica que o codec apresenta um certificado CS-Room emitido pela ACT2 SUDI CA (Organização: Cisco) com a cadeia de certificados terminando em Cisco Root CA 2048. O sistema de verificação de segurança relata isso como uma cadeia de certificados não confiáveis que não atende aos requisitos de segurança organizacionais.

As descobertas específicas relatadas pelas verificações de segurança incluem:

- Detecção de certificado autoassinado
- Cadeia de certificados não confiáveis
- Preocupações fracas com o algoritmo de dispersão
- Avisos de expiração de certificado

Ambiente

- Endpoints de codec de vídeo Cisco Telepresence
- Dispositivos Webex Desk Series com registro no local
- Endpoints com chips ACT2 SUDI (Secure Unique Device Identifier)
- Problemas da cadeia de certificados de sinalização da infraestrutura de verificação de

vulnerabilidades de segurança

- As portas TCP 4053, 4060 e 4062 que apresentam certificados SUDI

Resolução

Os certificados SUDI nos endpoints do Cisco Telepresence são certificados incorporados e imutáveis que não podem ser modificados, regenerados ou excluídos de uma maneira suportada. Esses certificados fazem parte da implementação de tecnologias confiáveis da Cisco e atendem a funções de segurança específicas.

Entendendo o comportamento do certificado SUDI

O comportamento do certificado varia de acordo com a porta e a configuração do sistema:

- Porta 4053 (Serviço de Emparelhamento): Usa certificados SUDI quando o sistema tem um chip ACT2. Os certificados personalizados são usados apenas em sistemas sem um chip ACT2 (endpoints mais antigos).
- Porta 4047: Usa certificados escolhidos pelo cliente para comunicação entre painéis sensíveis ao toque e codecs.

Localização e detalhes do certificado

Os certificados SUDI estão localizados no armazenamento de certificados do 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
```

Os detalhes do certificado ACT2 SUDI CA:

```
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
```

Ações recomendadas

Passo 1: Revisar a finalidade do certificado SUDI e a implementação da segurança

O certificado SUDI não é autoassinado, mas é assinado pela CA de fabricação Cisco. Ele serve como uma credencial de identidade imutável que:

- Mantém o identificador e o número de série do produto
- Fornece identidade inalterável para configuração, segurança, auditoria e gerenciamento
- Está ligado criptograficamente ao chip do módulo Âncora de Confiança
- Torna a clonagem ou a falsificação praticamente impossível

Passo 2: Trabalhar com a equipe de segurança para excluir as descobertas do certificado SUDI

Uma vez que os certificados SUDI não podem ser modificados e servem funções de segurança legítimas, a abordagem recomendada é:

- Configurar ferramentas de verificação de segurança para excluir as descobertas da cadeia de certificados SUDI para os serviços afetados
- Documentar a justificativa comercial para a exceção com base na implementação de tecnologias confiáveis da Cisco
- Concentre a verificação de segurança em certificados configuráveis pelo cliente em outras portas, se necessário

Passo 3: Atualizações de certificado por meio de atualizações de software

As atualizações de certificado no armazenamento confiável ocorrem automaticamente quando o

sistema é atualizado para versões de software mais recentes. Isso garante que a validade do certificado seja mantida ao longo do tempo.

Limitações importantes

Estas limitações aplicam-se aos certificados SUDI:

- Não pode ser modificado, regenerado ou excluído
- A regeneração automática ocorrerá se os certificados forem excluídos e o dispositivo for reiniciado
- Não existe nenhum método suportado para atribuir certificados configuráveis a estes serviços de backend
- A substituição de certificado não é possível devido à natureza imutável da implementação da Âncora de Confiança

Causa

As descobertas da verificação de segurança são disparadas pela presença de certificados SUDI (Secure Unique Device Identifier) da Cisco, que são certificados de fabricação integrados que se enquadram no Cisco Root CA 2048. Esses certificados fazem parte da implementação de tecnologias confiáveis da Cisco e foram projetados para serem imutáveis por motivos de segurança. Os certificados não são reconhecidos como confiáveis pelas ferramentas de verificação de segurança organizacional porque terminam na autoridade de certificação raiz da Cisco, em vez de em uma CA específica da organização. Este é o comportamento esperado para dispositivos habilitados para SUDI e representa um recurso de design em vez de uma vulnerabilidade de segurança.

Conteúdo relacionado

- Especificações da Cisco Trustworthy Technologies
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.