Risolvere i problemi relativi ai risultati dell'analisi della sicurezza della catena di certificati SUDI Telepresence

Sommario

Problema

Le analisi delle vulnerabilità di sicurezza segnalano i risultati relativi ai certificati SSL/TLS sugli endpoint di codec video Cisco Telepresence, segnalando in particolare una catena di certificati non attendibili sulle porte TCP 4053, 4060 e 4062. Lo scanner di vulnerabilità identifica il codec che presenta un certificato CS-Room rilasciato da ACT2 SUDI CA (Organizzazione: Cisco) con la catena di certificati che termina alla CA radice Cisco 2048. Il sistema di analisi di protezione segnala questa situazione come una catena di certificati non attendibile che non soddisfa i requisiti di protezione dell'organizzazione.

I risultati specifici segnalati dalle scansioni di sicurezza includono:

- Rilevamento certificati autofirmati
- Catena di certificati non attendibili
- Problemi relativi all'algoritmo hash debole
- Avvisi di scadenza certificato

Ambiente

- Cisco Telepresence Video Codec Endpoint
- Dispositivi della serie Webex Desk con registrazione locale
- Endpoint con chip ACT2 SUDI (Secure Unique Device Identifier)
- Sicurezza vulnerabilità analisi infrastruttura contrassegno problemi catena di certificati

- porte TCP 4053, 4060 e 4062 che presentano certificati SUDI

Risoluzione

I certificati SUDI sugli endpoint Cisco Telepresence sono certificati incorporati e non modificabili che non possono essere modificati, rigenerati o eliminati in modo supportato. Questi certificati fanno parte dell'implementazione di Cisco Trusted Technologies e svolgono funzioni di sicurezza specifiche.

Informazioni sul comportamento dei certificati SUDI

Il comportamento del certificato varia a seconda della porta e della configurazione del sistema:

- Port 4053 (Servizio di accoppiamento): Utilizza i certificati SUDI quando il sistema dispone di un chip ACT2. I certificati personalizzati vengono utilizzati solo nei sistemi senza un chip ACT2 (endpoint precedenti).
- Porta 4047: Utilizza i certificati scelti dal cliente per la comunicazione tra touch panel e codec.

Percorso e dettagli del certificato

I certificati SUDI si trovano nell'archivio certificati 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
```

Dettagli del certificato 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
```

Azioni consigliate

Passaggio 1: Verifica lo scopo del certificato SUDI e l'implementazione della protezione

Il certificato SUDI non è autofirmato ma è firmato dalla CA di Cisco Manufacturing. Funge da credenziale di identità non modificabile che:

- Gestisce l'identificativo del prodotto e il numero di serie
- Fornisce un'identità immutabile per la configurazione, la sicurezza, il controllo e la gestione
- È associato crittograficamente al chip del modulo Trust Anchor
- Clonazione e spoofing praticamente impossibili

Passaggio 2: Collaborare con il team di sicurezza per escludere i risultati dei certificati SUDI

Poiché i certificati SUDI non possono essere modificati e svolgono funzioni di sicurezza legittime, l'approccio consigliato è il seguente:

- Configurare gli strumenti di analisi della sicurezza per escludere i risultati della catena di certificati SUDI per i servizi interessati
- Documentare la motivazione aziendale per l'eccezione in base all'implementazione di Cisco Trustworthy Technologies
- Concentrare l'analisi di protezione su certificati configurabili dal cliente su altre porte, se necessario

Passaggio 3: Aggiornamenti dei certificati tramite aggiornamenti software

Gli aggiornamenti dei certificati nell'archivio di attendibilità vengono eseguiti automaticamente quando il sistema viene aggiornato alle nuove versioni del software. In questo modo si garantisce che la validità del certificato venga mantenuta nel tempo.

Limitazioni importanti

Ai certificati SUDI si applicano le limitazioni seguenti:

- Impossibile modificare, rigenerare o eliminare
- La rigenerazione automatica viene eseguita se i certificati vengono eliminati e il dispositivo viene riavviato
- Non esiste alcun metodo supportato per assegnare certificati configurabili a questi servizi back-end
- La sostituzione del certificato non è possibile a causa della natura immutabile dell'implementazione del trust anchor

Causa

I risultati dell'analisi della sicurezza sono attivati dalla presenza dei certificati SUDI (Secure Unique Device Identifier) di Cisco, ovvero certificati di produzione incorporati concatenati alla CA radice Cisco 2048. Questi certificati fanno parte dell'implementazione di Cisco Trusted Technologies e sono progettati per essere immutabili per motivi di sicurezza. I certificati non vengono riconosciuti come attendibili dagli strumenti di analisi della sicurezza dell'organizzazione perché terminano presso l'autorità di certificazione principale di Cisco anziché presso una CA specifica dell'organizzazione. Si tratta di un comportamento previsto per i dispositivi abilitati per SUDI e rappresenta una caratteristica di progettazione piuttosto che una vulnerabilità di sicurezza.

Contenuto correlato

- Tecnologie Attendibili Cisco
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).