Aggiornamento di AsyncOS for Email Security versione 9.5 e successive con certificati precedenti (MD5) e comunicazione TLSv1.2 non riuscita

Sommario

Introduzione

In questo documento vengono descritti i passaggi necessari da eseguire in caso di problemi di comunicazione TLS o di accesso all'interfaccia Web dopo l'aggiornamento a AsyncOS for Email Security versione 9.5 o successive su Cisco Email Security Appliance (ESA).

I certificati legacy (MD5) impediscono la comunicazione con TLSv1.2 su AsyncOS 9.5 per gli aggiornamenti di Email Security e versioni successive

> **Nota:** Di seguito è riportata una soluzione alternativa per i certificati demo correnti applicati all'accessorio. Tuttavia, i passaggi seguenti possono essere applicati anche a tutti i certificati MD5 firmati.

Quando si esegue un aggiornamento a AsyncOS for Email Security versione 9.5 e successive, uno qualsiasi dei certificati demo IronPort legacy ancora in uso e applicati per la consegna, la ricezione o il protocollo LDAP, potrebbe riscontrare errori durante il tentativo di comunicazione tramite TLSv1/TLSv1.2 con alcuni domini. L'errore TLS provocherà un errore in tutte le sessioni in entrata o in uscita.

Se i certificati vengono applicati all'interfaccia HTTPS, i browser Web moderni non saranno in grado di accedere all'interfaccia Web dell'accessorio.

I log di posta dovrebbero essere simili all'esempio seguente:

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
```

Questo errore è causato dall'algoritmo di firma applicato al certificato precedente che è MD5. tuttavia, i certificati associati all'accessorio o al browser di connessione supportano solo algoritmi basati su firma SHA. Sebbene i certificati demo meno recenti con firma MD5 siano presenti sull'accessorio contemporaneamente al nuovo certificato demo basato su Agente integrità sistema, l'errore precedente si manifesterà solo se il certificato basato su firma MD5 viene applicato alle sezioni specificate (ad esempio ricezione, consegna, ecc.)

Di seguito è riportato un esempio estratto dalla cli di un accessorio che dispone sia dei certificati MD5 precedenti sia del nuovo certificato demo (nota: il certificato più recente (Demo) deve essere il più recente dell'algoritmo SHA e avere una data di scadenza più lunga rispetto ai certificati demo meno recenti.

```
List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
delivery_  IronPort Appliance D  IronPort Appliance D  Active          303 days
https_cer  IronPort Appliance D  IronPort Appliance D  Active          303 days
ldaps_cer  IronPort Appliance D  IronPort Appliance D  Active          303 days
receiving  IronPort Appliance D  IronPort Appliance D  Valid           303 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3218 days
```

Azioni correttive

1. Passare al Web (UI): **Rete > Certificati**
2. Verificare che siano installati i certificati meno recenti e che sia installato il nuovo certificato demo SHA.
3. In base alla posizione in cui vengono applicati i certificati demo meno recenti, sostituirlo con un nuovo certificato demo.

In genere questi certificati vengono applicati nelle sezioni seguenti:

- **Rete > Listener > Nome del listener > Certificato**
- **Criteri di posta > Controlli destinazione > Modifica impostazioni globali > Certificato**
- **Rete > Interfaccia IP > Scegli interfaccia associata con accesso GUI > Certificato HTTPS**
- **Amministrazione sistema > LDAP > Modifica impostazioni > Certificato**

4. Dopo aver sostituito tutti i certificati, verificare dalla riga di comando che la comunicazione TLS sia stata eseguita correttamente.

Esempio di comunicazione TLS funzionante negoziata utilizzando TLSv1.2:

```
Thu Jul  2 16:38:30 2015 Info: New SMTP ICID 4435675 interface Data1 (10.0.10.1)
address 209.85.213.182 reverse dns host mail-ig0-f182.google.com verified yes Thu Jul 2 16:38:30
2015 Info: ICID 4435675 ACCEPT SG UNKNOWNLIST match sbrs[0.0:10.0] SBRS 4.8 Thu Jul 2 16:38:30
2015 Info: ICID 4435675 TLS success protocol TLSv1.2 cipher AES128-GCM-SHA256
```

Azioni correttive CLI (se non è possibile accedere alla GUI)

Potrebbe essere necessario modificare il certificato in ogni interfaccia IP in cui è abilitato un certificato per il servizio HTTPS. Per modificare il certificato in uso per le interfacce, eseguire i seguenti comandi dalla CLI:

1. Digitare **interfaceconfig**.
2. Selezionare **Modifica**.
3. Immettere il numero dell'interfaccia che si desidera modificare.
4. Utilizzare il tasto Invio per accettare le impostazioni correnti per ciascuna domanda presentata. Quando viene visualizzata l'opzione per il certificato da applicare, selezionare il certificato demo:
   1.
   ```
   1. Ironport Demo Certificate
   2. Demo
   Please choose the certificate to apply:
   [1]> 2

   You may use "Demo", but this will not be secure.
   Do you really wish to use the "Demo" certificate? [N]> Y
   ```
5. Completare le istruzioni dettagliate delle richieste di impostazioni fino al completamento di tutte le domande sulla configurazione.
6. Usare il tasto Return per uscire dal prompt CLI principale.
7. **Utilizzare il comando commit** per salvare le modifiche apportate alla configurazione.

Nota: ricordarsi di eseguire il **commit** delle modifiche dopo aver modificato il certificato in uso nell'interfaccia.

Informazioni correlate

- Guida completa alla configurazione di TLS su ESA
- Cisco Email Security Appliance - Guide per l'utente
- Cisco Security Management Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems