9.5 en nieuwere AsyncOS voor e-mail security upgrade met oudere certificaten (MD5) communicatie-TLSv1.2 om te falen

Inhoud

Inleiding

Dit document beschrijft de gewenste stappen die moeten worden toegepast bij het tegenkomen van een probleem met de TLS-communicatie of bij het bereiken van de web-interface, na het upgraden naar AsyncOS voor e-mail security versie 9.5 of nieuwer op Cisco e-mail security applicaties (ESA).

Verouderde certificaten (MD5) veroorzaken dat de communicatie met TLSv1.2 mislukt op 9.5 AsyncOS voor e-mail security upgrades en nieuwere

> Opmerking: Hieronder vindt u een lijst met opties voor de huidige demonstratiecertificaten die op het apparaat worden toegepast. De volgende stappen kunnen echter ook van toepassing zijn op alle door de MD5 ondertekende certificaten.

Na het uitvoeren van een upgrade naar AsyncOS voor e-mail security versie 9.5 en nieuwer, kan een van de bestaande IronPort-demo-certificaten die nog in gebruik zijn en voor levering, ontvangst of LDAP zijn aangevraagd, fouten ervaren bij het communiceren via TLSv1/TLSv1.2 met een aantal domeinen. De TLS fout zal alle inkomende of uitgaande sessies laten mislukken.

Als de certificaten worden toegepast op de HTTPS-interface, hebben moderne webbrowsers geen toegang tot de webinterface van het apparaat.

De logbestanden van de post zouden op het volgende voorbeeld moeten lijken:

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

Deze fout wordt veroorzaakt door het algoritme van de handtekening toegepast op het oudere certificaat, zijnde MD5. de certificaten die gekoppeld zijn aan het verbindingsapparaat/browser

ondersteunen echter alleen op SHA gebaseerde algoritmen. Hoewel de oudere demo-certificaten met de MD5-handtekening op het apparaat zijn aangebracht op hetzelfde moment dat het nieuwe SHA-demo-certificaat de bovenstaande fout alleen vertoont als het op de MD5 gebaseerde certificaat voor handtekening wordt toegepast op de gespecificeerde onderdelen (d.w.z. ontvangst, levering, enz.).

Hieronder vindt u een voorbeeld dat is getrokken uit de cloud van een apparaat dat zowel de oudere MD5-certificaten heeft in aanvulling op het nieuwe Demo-certificaat (opmerking: het nieuwere certificaat (Demo) moet het nieuwere SHA-algoritme zijn en een langere vervaldatum hebben dan de oudere demo-certificaten):

```
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
```

Correctieve maatregelen

1. Navigeren naar het web (UI): **Network > Certificaten**
2. Controleer of de oudere certificaten op dit moment zijn geïnstalleerd en gebruik ook het nieuwe SHA Demo-certificaat.
3. Gebaseerd op de plaats waar de oudere demo certificaten worden toegepast vervang dit door het nieuwe Demo certificaat.

Deze certificaten worden doorgaans in de volgende delen toegepast:

- **Netwerk > Lijsten > Naam van de luisteraar > Certificaat**
- **Mail Polities > Destination Control > Global Settings > certificaataanvraag**
- **Network > IP-interface > Kies een interface die is gekoppeld aan GUI-toegang > HTTPS-certificaat**
- **Systeembeheer > LDAP > Instellingen bewerken > Certificaat**

4. Nadat alle certificaten zijn vervangen, controleert u vanuit de opdrachtregel of de TLS-communicatie nu succesvol is.

Voorbeeld van een werkende TLS-communicatie waarover met behulp van TLSv1.2 wordt onderhandeld:

```
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
```

CLI-corrigerende maatregelen (indien GUI niet benaderd kan worden)

Het certificaat moet mogelijk worden aangepast op elke IP-interface met een certificaat dat is ingeschakeld voor HTTPS-service. U kunt het certificaat dat voor interfaces wordt gebruikt, als

volgt wijzigen: voert u de volgende opdrachten uit op de CLI:

1. Type **interfaceconfig**.
2. Selecteer **Bewerken**.
3. Typ het nummer van de interface dat u wilt bewerken.
4. Gebruik de retourtoets om de huidige instellingen voor elke gepresenteerde vraag te aanvaarden. Selecteer bij de presentatie van de optie voor het toe te passen certificaat het demo-certificaat:
   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. Voltooien van de instellingen leidt tot alle configuratievragen zijn voltooid.
6. Gebruik de retour-toets om de hoofdCLI-melding te verlaten.
7. **Gebruik deze optie** om de wijzigingen in de configuratie op te slaan.

Opmerking: vergeet wijzigingen aan te **leggen** nadat u het certificaat dat op de interface wordt gebruikt, hebt gewijzigd.

Gerelateerde informatie

- Comprehensive Setup Guide voor TLS op ESA
- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Cisco Security Management-applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems