9.5 und neuere AsyncOS für Email Security-Upgrade mit älteren Zertifikaten (MD5), TLSv1.2-Kommunikation fehlschlägt

Inhalt

Einführung

In diesem Dokument werden die erforderlichen Schritte beschrieben, die nach dem Upgrade auf AsyncOS für Email Security 9.5 oder höher auf den Cisco Email Security Appliances (ESA) bei einem Problem mit der TLS-Kommunikation oder dem Zugriff auf die Webschnittstelle anzuwenden sind.

Legacy-Zertifikate (MD5) führen zu einem Ausfall der TLSv1.2-Kommunikation unter 9.5 AsyncOS für E-Mail-Security-Upgrades und neuere Versionen.

> **Hinweis**: Im Folgenden finden Sie eine Problemumgehung für die aktuellen Demo-Zertifikate, die auf der Appliance angewendet werden. Die folgenden Schritte können jedoch auch für alle MD5-signierten Zertifikate verwendet werden.

Bei der Durchführung eines Upgrades auf AsyncOS für E-Mail-Sicherheit Version 9.5 und höher können bei allen Legacy-IronPort-Demo-Zertifikaten, die noch in Gebrauch sind und für die Zustellung, den Empfang oder das LDAP angewendet werden, Fehler auftreten, wenn versucht wird, über TLSv1/TLSv1.2 mit einigen Domänen zu kommunizieren. Der TLS-Fehler führt dazu, dass alle ein- oder ausgehenden Sitzungen fehlschlagen.

Wenn die Zertifikate auf die HTTPS-Schnittstelle angewendet werden, können moderne Webbrowser nicht auf die Webschnittstelle der Appliance zugreifen.

Mail-Protokolle sollten ähnlich wie im folgenden Beispiel aussehen:

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

Dieser Fehler wird durch den Signaturalgorithmus verursacht, der auf das ältere Zertifikat MD5

angewendet wird. Allerdings unterstützen die Zertifikate, die der verbundenen Appliance/dem Browser zugeordnet sind, nur SHA-signaturbasierte Algorithmen. Obwohl sich die älteren Demozertifikate, die über die MD5-Signatur verfügen, auf der Appliance gleichzeitig das neue SHA-basierte Demozertifikat befinden, wird der obige Fehler nur auftreten, wenn das signaturbasierte MD5-Zertifikat auf die angegebenen Abschnitte (d. h. Empfang, Lieferung usw.) angewendet wird.

Im Folgenden sehen Sie ein Beispiel, das von der CLI einer Appliance gezogen wird, die neben dem neuen Demozertifikat über beide älteren MD5-Zertifikate verfügt (Hinweis: Das neuere Zertifikat (Demo) sollte der neuere SHA-Algorithmus sein und ein längeres Ablaufdatum als die älteren Demo-Zertifikate haben.):

```
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
```

Korrekturmaßnahmen

1. Navigieren Sie zum Web (UI): **Netzwerk > Zertifikate**
2. Stellen Sie sicher, dass Sie aktuell die älteren Zertifikate installiert haben und außerdem über das neue SHA Demo-Zertifikat verfügen.
3. Je nachdem, wo die älteren Demo-Zertifikate angewendet werden, wird dies durch ein neues Demo-Zertifikat ersetzt.

In der Regel werden diese Zertifikate in den folgenden Abschnitten angewendet:

- **Netzwerk > Listener > dann name of the Listener > Certificate**
- **Mail-Policys > Zielsteuerelemente > Globale Einstellungen bearbeiten > Zertifikat**
- **Netzwerk > IP-Schnittstelle > Schnittstelle für GUI-Zugriff auswählen > HTTPS-Zertifikat**
- **Systemverwaltung > LDAP > Einstellungen bearbeiten > Zertifikat**

4. Nachdem alle Zertifikate ausgetauscht wurden, stellen Sie sicher, dass die TLS-Kommunikation jetzt erfolgreich ist.

Beispiel für die funktionierende TLS-Kommunikation, die mit TLSv1.2 ausgehandelt wird:

```
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-Korrekturmaßnahmen (wenn auf die GUI nicht zugegriffen werden kann)

Das Zertifikat muss möglicherweise auf jeder IP-Schnittstelle geändert werden, für die ein für den HTTPS-Dienst aktiviertes Zertifikat aktiviert ist. Führen Sie die folgenden Befehle in der CLI aus, um das für Schnittstellen verwendete Zertifikat zu ändern:

1. Geben Sie **interfaceConfig ein**.
2. Wählen Sie **Bearbeiten aus**.
3. Geben Sie die Nummer der Schnittstelle ein, die Sie bearbeiten möchten.
4. Akzeptieren Sie mit dem Rückgabetasten die aktuellen Einstellungen für jede gestellte Frage. Wenn die Option zur Anwendung des Zertifikats angezeigt wird, wählen Sie das Demozertifikat aus:
   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. Führen Sie die einzelnen Schritte durch, bis alle Konfigurationsfragen abgeschlossen sind.
6. Beenden Sie die CLI-Eingabeaufforderung mit der Rückgabetaste.
7. **Mit "Übernehmen"** speichern Sie Ihre Änderungen in der Konfiguration.

Hinweis: Bitte denken Sie daran, Änderungen **zu bestätigen**, nachdem Sie das auf der Schnittstelle verwendete Zertifikat geändert haben.

Zugehörige Informationen

- Umfassender Einrichtungsleitfaden für TLS auf ESA
- Cisco Email Security Appliance - Benutzerhandbücher
- Cisco Security Management Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems