電子メール セキュリティ用の AsyncOS 9.5 以降を古い証明書（MD5）でアップグレードすると TLSv1.2 通信が失敗する

目次

概要

この文書は場合適用されるべき必要な ステップを記述したものです TLS コミュニケーションにおいての問題に出会っているか、または Webインターフェイスに、Cisco E メール セキュリティ アプライアンス（ESA）の E メール セキュリティ バージョン 9.5 または それ 以降のための AsyncOS へのアップグレードした後でアクセスします。

E メール セキュリティ アップグレードのための 9.5 AsyncOS で失敗するレガシー証明書（MD5）原因 TLSv1.2 コミュニケーションおよびより新しい

> **注:** 以下は機器で加えられる現在のデモ 証明書のためのリストされた対応策です。 ただし、下記のステップはまたあらゆる MD5 署名入り認証に機器適用されるかもしれません。

E メール セキュリティ バージョン 9.5 および それ 以降のための AsyncOS へのアップグレードを、配達のために、受け取るか、または LDAP 使用中および応用、レガシー IronPort デモ 証明書のうちのどれかがまだ行った上でいくつかのドメインと TLSv1/TLSv1.2 によって通信することを試みている間エラーを経験するかもしれません。 TLS エラーによりすべての受信かアウトバウンド セッションは失敗します。

証明書が HTTPS インターフェイスに加えられる場合、現代 Webブラウザは機器の Webインターフェイスにアクセスしません。

メール ログは次の例に類似したに検知 する必要があります:

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

このエラーは MD5 であるより古い証明書に適用されるシグニチャ アルゴリズムによって引き起こされます; ただし、機器/ブラウザの接続と関連付けられる証明書は SHA シグニチャによって基

づくアルゴリズムだけをサポートします。 、より古いデモ 証明書が機器に持っている MD5 シグ二チャ同じ時間新しい SHA によって基づくデモ 証明書であるが上記のエラーは MD5 シグ二チャによって基づく証明書が規定 されたセクションに加えられる場合その時だけそれ自身を明示します (すなわち受信、配達、等)

新しいデモ 証明書 (注記に加えて両方のより古い MD5 証明書がある機器の cli から引っ張られる例は下記にあります: より新しい証明書 (デモ) ははずです SHA アルゴリズム新しいおよびより古いデモ 証明書より長い有効期限を過す) 。:

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

是正措置

1. Web （ UI) へのナビゲート: **ネットワーク > 証明書**
2.また新しい SHA デモ 証明書を持ちなさいことをことを現在インストールしてもらうより古い証明書を確認すれば。
3.基づいてより古いデモ 証明書が適用するどこににか新しいデモ 証明書とこれを取り替えて下さい。

通常これらの証明書は次のセクションで適用されることを見つけることができます:

- **ネットワーク > リスナー > そしてリスナー > 証明書の名前**
- **メールは > 宛先制御 > Edit グローバルな設定 > 証明書ポリシングを行ないます**
- **ネットワーク > IPインターフェイスは > GUIアクセス > HTTPS 証明書と関連付けられるインターフェイスを選択します**
- **システム 管理 > LDAP > Edit 設定 > 証明書**

4. すべての証明書が取り替えられたら TLS コミュニケーションが現在正常であることをコマンド・ラインから確認して下さい。

TLSv1.2 を使用してネゴシエートされる TLS 通信をはたらかせる例:

```
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
```

(GUI がアクセスすることができなければ) CLI 是正措置

HTTPS サービスのためにイネーブルになっている証明書がある証明書は各 IPインターフェイスで修正される必要がある場合もあります。 インターフェイスのために使用中の証明書を修正するために CLI の次のコマンドを実行して下さい:

1. interfaceconfig を入力して下さい。
2. 『Edit』 を選択 して下さい。
3. 編集したいインターフェイスの数を入力して下さい。
4. 示される各質問の現在の設定を受け入れるのにリターン キーを使用して下さい。 適用するべき証明書のためのオプションが示されるとき、デモ 証明書を選択して下さい:
    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. すべてのコンフィギュレーションに関する質問が完了するまで設定プロンプトによって歩むことを終えて下さい。
6. 主要な CLI プロンプトに終了するのにリターン キーを使用して下さい。
7. 設定への変更を保存する Usecommit。

注: インターフェイスで使用中の証明書を変更した後変更を**保存することを**忘れないようにして下さい。

関連情報

- ESA での TLS 向けの包括的な設定ガイド
- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- Cisco セキュリティ管理アプライアンス - エンドユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems