9.5 et plus nouvel AsyncOS pour la mise à jour de sécurité du courrier électronique avec une transmission plus ancienne TLSv1.2 de Certificats (MD5) à échouer

Contenu

Introduction
Transmission existante de la cause TLSv1.2 de Certificats (MD5) à échouer sur 9.5 AsyncOS pour des mises à jour de sécurité du courrier électronique et plus nouveau
Actions correctives
Actions correctives CLI (si le GUI ne peut pas être accédé à)
Informations connexes
Cisco relatif prennent en charge des discussions de la Communauté

Introduction

Ce document décrit les étapes nécessaires à appliquer si rencontrant une question avec la transmission de TLS, ou accédant à l'interface de Web, après évolution à AsyncOS pour la version 9.5 ou plus récentes de sécurité du courrier électronique sur les appliances de sécurité du courrier électronique de Cisco (ESA).

Transmission existante de la cause TLSv1.2 de Certificats (MD5) à échouer sur 9.5 AsyncOS pour des mises à jour de sécurité du courrier électronique et plus nouveau

> Remarque: Ce qui suit est un contournement énuméré pour les Certificats en cours de démonstration appliqués sur l'appliance. Cependant, les étapes ci-dessous peuvent également appliance s'appliquer à tous les Certificats signés de MD5.

En exécutant une mise à jour à AsyncOS pour la version 9.5 et plus récentes de sécurité du courrier électronique, les Certificats existants l'uns des de démonstration d'IronPort encore en service et appliqués pour la livraison, réception ou LDAP, peuvent éprouver des erreurs tout en essayant de communiquer par l'intermédiaire de TLSv1/TLSv1.2 avec quelques domaines. L'erreur de TLS fera échouer toutes les sessions d'arrivée ou sortantes.

Si les Certificats sont appliqués à l'interface HTTPS, les navigateurs Web modernes n'accéderont à pas l'interface web de l'appliance.

Les logs de messagerie devraient sembler semblables à l'exemple suivant :

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

Cette erreur est provoqué par par l'algorithme de signature appliqué au certificat plus ancien étant MD5 ; cependant, les Certificats associés avec l'appliance/navigateur se connectants prennent en charge seulement les algorithmes basés par signature de SHA. Bien que, les Certificats plus anciens de démonstration qui a la signature de MD5 soient sur l'appliance le même temps le certificat de démonstration basé nouveau par SHA l'erreur ci-dessus se manifestera seulement si le certificat basé par signature de MD5 est appliqué aux sections spécifiées (c.-à-d. réception, livraison, etc.)

Est ci-dessous un exemple tiré du cli d'une appliance qui a les les deux les Certificats plus anciens de MD5 en plus du nouveau certificat de démonstration (note : le certificat plus nouveau (démonstration) devrait être plus l'algorithme de SHA et avoir une plus longue date d'expiration que les Certificats plus anciens de démonstration) est nouveau. :

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

Actions correctives

1. Naviguez vers le Web (UI) : **Réseau > Certificats**
2. Vérifiez que vous font actuellement installer les Certificats plus anciens et ayez également le nouveau certificat de démonstration de SHA.
3. Basé sur où les Certificats plus anciens de démonstration sont appliqués remplacez ceci par le nouveau certificat de démonstration.

Typiquement ces Certificats peuvent être application trouvée dans les sections suivantes :

- **Réseau > auditeurs > puis nom de l'auditeur > du certificat**
- **La messagerie maintient l'ordre > des contrôles de destination > éditent les paramètres généraux > le certificat**
- **Le réseau > l'interface IP > choisissent l'interface associée avec l'accès GUI > le certificat HTTPS**
- **L'administration système > le LDAP > éditent les configurations > le certificat**

4. Une fois que tous les Certificats ont été remplacés vérifiez de la ligne de commande que la transmission de TLS est maintenant réussie.

Exemple de fonctionner la transmission de TLS étant négociée utilisant 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
```

Actions correctives CLI (si le GUI ne peut pas être accédé à)

Le certificat peut devoir être modifié sur chaque interface IP qui a un certificat activé pour le service HTTPS. Afin de modifier le certificat en service pour des interfaces, exécutez s'il vous plaît les commandes suivantes sur le CLI :

1. **Interfaceconfig de** type.
2. Select **éditent**.
3. Introduisez le nombre de l'interface que vous souhaitez éditer.
4. Employez la clé de retour pour recevoir les configurations actuelles pour chaque question présentée. Quand l'option pour que le certificat s'applique est présentée, sélectionnez le certificat de démonstration :

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. La finition faisant un pas par les configurations incite jusqu'à ce que toutes les questions relatives à la configuration soient terminées.
6. Employez la clé de retour pour quitter à la demande principale CLI.
7. Usecommit pour sauvegarder vos modifications à la configuration.

Remarque: Souvenez-vous s'il vous plaît **pour commettre des** modifications après avoir changé le certificat en service sur l'interface.

Informations connexes

- Guide complet d'installation pour le TLS sur l'ESA
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Appliance de Gestion de sécurité Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems