Empêchez les négociations pour des chiffrements nuls ou anonymes sur l'ESA et le SMA

ID de document : 117864

Mis à jour : FÉV 19, 2015

Contribué par l'ouïe et le Robert Sherwin de Jai, ingénieurs TAC Cisco.

PDF de téléchargement
Copie
Commentaires

Produits connexes

- Appliance de sécurité du courrier électronique de Cisco

Contenu

Introduction

Ce document décrit comment les configurations de chiffrement modifier de Cisco de sécurité du courrier électronique appareils (ESA) et d'appareils de Gestion de sécurité Cisco (SMA) afin d'empêcher des négociations pour des chiffrements nuls ou anonymes. Ce document s'applique aux appliances basées basées et virtuelles de matériel.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ESA
- Cisco SMA

Composants utilisés

Les informations dans ce document sont basées sur toutes les versions de Cisco ESA et de Cisco SMA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Empêchez les négociations pour des chiffrements nuls ou anonymes

Cette section décrit comment empêcher des négociations pour des chiffrements nuls ou anonymes sur Cisco ESA qui exécute AsyncOS pour des versions 9.1 et ultérieures de sécurité du courrier électronique, et également sur Cisco SMA.

ESAs ce passage AsyncOS pour la version 9.1 ou ultérieures de sécurité du courrier électronique

Vous pouvez modifier les chiffrements qui sont utilisés sur l'ESA avec la commande de **sslconfig**. Afin d'empêcher les négociations ESA pour des chiffrements nuls ou anonymes, sélectionnez la commande de **sslconfig** dans l'ESA CLI et appliquez ces configurations :

- Méthode d'arrivée de Protocole SMTP (Simple Mail Transfer Protocol) : **sslv3tlsv1**
- Chiffrements d'arrivée de SMTP : **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**
- Méthode sortante de SMTP : **sslv3tlsv1**
- Chiffrements sortants de SMTP : **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**

Voici un exemple de configuration pour des chiffrements d'arrivée :

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
```

```
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit inbound SMTP ssl settings.
- OUTBOUND - Edit outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

> Remarque: Placez le **GUI**, **D'ARRIVÉE**, et **SORTANT** comme nécessaire pour chaque chiffrement.

En date d'AsyncOS pour la version 8.5 de sécurité du courrier électronique, la commande de **sslconfig** est également disponible par l'intermédiaire du GUI. Afin d'atteindre ces configurations du GUI, naviguez vers l'**administration système > les configurations SSL > éditent des configurations** :

> **Conseil** : Sécurisez les sockets que la version 3.0 (RFC-6101) du varech (SSL) est une Désuet(e) et un protocole non sécurisé. Il y a une vulnérabilité dans SSLv3 CVE-2014-3566 connu sous le nom de *compléter Oracle sur l'attaque existante de cryptage Downgraded (CANICHE)*, qui est dépistée par l'ID de bogue Cisco CSCur27131. Cisco recommande que vous désactiviez SSLv3 tandis que vous changez les chiffrements, utilisez le Transport Layer Security (TLS) seulement, et sélectionnez l'*option 3* (TLS v1). Référez-vous à l'ID de bogue Cisco CSCur27131 pour les détails complets.

ESAs ce passage AsyncOS pour la version 9.5 ou ultérieures de sécurité du courrier électronique

Avec l'introduction d'AsyncOS pour la version 9.5 de sécurité du courrier électronique, le TLS v1.2 est maintenant pris en charge. Les commandes qui sont encore décrites dans la section précédente fonctionnent ; cependant, vous verrez les mises à jour pour le TLS v1.2 inclus dans les sorties.

Voici un exemple de sortie du CLI :

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
```

```
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>
```

Afin d'atteindre ces configurations du GUI, naviguez vers l'**administration système > la configuration SSL > éditent des configurations…** :

> **Conseil** : Pour les informations complètes, référez-vous au guide approprié d'utilisateur ESA pour la version 9.5 ou ultérieures.

SMA

La commande de **sslconfig** n'est pas disponible pour Cisco SMA.

> Remarque: À ce moment, seulement le TLS v1 est pris en charge ; Le TLS v1.2 est seulement pris en charge sur l'ESA.

Vous devez se terminer ces étapes du SMA CLI afin de modifier les chiffrements SSL :

1. Sauvegardez le fichier de configuration SMA à votre ordinateur local.
2. Ouvrez le fichier XML.
3. Recherchez la section de *<ssl>* dans le XML :
   ```
   <ssl>
   ```

```
    <ssl_inbound_method>sslv3tlsv1</ssl_inbound_method>
    <ssl_inbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_inbound_ciphers>
    <ssl_outbound_method>sslv3tlsv1</ssl_outbound_method>
    <ssl_outbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_outbound_ciphers>
    <ssl_gui_method>sslv3tlsv1</ssl_gui_method>
    <ssl_gui_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_gui_ciphers>
  </ssl>
```

4. Modifiez les chiffrements comme désirés et sauvegardez le XML :

```
<ssl>
<ssl_inbound_method>tlsv1</ssl_inbound_method>
<ssl_inbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_inbound_ciphers>
<ssl_outbound_method>tlsv1</ssl_outbound_method>
<ssl_outbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_outbound_ciphers>
<ssl_gui_method>tlsv1</ssl_gui_method>
<ssl_gui_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_gui_ciphers>
</ssl>
```

5. Chargez le nouveau fichier de configuration sur le SMA.

6. **Soumettez** et **commettez** toutes les modifications.

Cisco relatif prennent en charge des discussions de la Communauté

Mis à jour : FÉV 19, 2015
ID de document : 117864