Prevenga las negociaciones para las cifras nulas o anónimas en el ESA y el S A

ID del Documento: 117864

Actualizado: De febrero el 19 de 2015

Contribuido por la papada y Roberto Sherwin de Jai, ingenieros de Cisco TAC.

Descarga PDF
Imprimir
Comentarios

Productos Relacionados

- Dispositivo de seguridad del correo electrónico de Cisco

Contenido

Introducción

Este documento describe cómo alterar las configuraciones de la cifra del dispositivo de seguridad del correo electrónico de Cisco (ESA) y del dispositivo de la Administración del Cisco Security (S A) para prevenir las negociaciones para las cifras nulas o anónimas. Este documento se aplica a los dispositivos basados basados y virtuales del hardware.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ESA
- Cisco S A

Componentes Utilizados

La información en este documento se basa en todas las versiones de Cisco ESA y de Cisco S A.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Prevenga las negociaciones para las cifras nulas o anónimas

Esta sección describe cómo prevenir las negociaciones para las cifras nulas o anónimas en Cisco ESA que ejecuta AsyncOS para las versiones 9.1 de la Seguridad del correo electrónico y posterior, y también en Cisco S A.

ESA que ejecutan AsyncOS para la versión 9.1 o posterior de la Seguridad del correo electrónico

Usted puede modificar las cifras que se utilizan en el ESA con el comando del **sslconfig**. Para prevenir las negociaciones ESA para las cifras nulas o anónimas, ingrese el comando del **sslconfig** en el ESA CLI y aplique estas configuraciones:

- Método entrante del Simple Mail Transfer Protocol (SMTP): **sslv3tlsv1**
- Cifras entrantes S TP: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**
- Método saliente S TP: **sslv3tlsv1**
- Cifras salientes S TP: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**

Aquí está un ejemplo de configuración para las cifras entrantes:

```
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
```

Nota: Fije el **GUI**, **ENTRANTE**, y **SALIENTE** según las necesidades para cada cifra.

A partir de AsyncOS para la versión 8.5 de la Seguridad del correo electrónico, el comando del **sslconfig** está también disponible vía el GUI. Para alcanzar estas configuraciones del GUI, navegue a la **administración del sistema > a las configuraciones de SSL > editan las configuraciones**:

Consejo: Asegure los socketes que el 3.0 de la versión del varec (SSL) (RFC-6101) es un Obsoleto y un protocolo inseguro. Hay una vulnerabilidad en SSLv3 CVE-2014-3566 conocido como *Oracle del relleno en el ataque del cifrado de la herencia Downgraded (CANICHE)*, que es seguido por el Id. de bug Cisco CSCur27131. Cisco recomienda que usted inhabilita SSLv3 mientras que usted cambia las cifras, utiliza Transport Layer Security (TLS) solamente, y selecciona el *option 3* (v1 de TLS). Refiera al Id. de bug Cisco CSCur27131 para los detalles completos.

ESA que ejecutan AsyncOS para la versión 9.5 o posterior de la Seguridad del correo electrónico

Con la introducción de AsyncOS para la versión 9.5 de la Seguridad del correo electrónico, el v1.2 de TLS ahora se soporta. Los comandos que todavía se describen en la sección anterior trabajan; sin embargo, usted verá las actualizaciones para el v1.2 de TLS incluido en las salidas.

Aquí está una salida de ejemplo del 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]>
```

Para alcanzar estas configuraciones del GUI, navegue a la **administración del sistema > a la configuración de SSL > editan las configuraciones…**:

> Consejo: Para la Información completa, refiera a la guía del usuario final apropiada ESA para la versión 9.5 o posterior.

S A

El comando del **sslconfig** no está disponible para Cisco S A.

> Nota: Ahora, solamente se soporta el v1 de TLS; El v1.2 de TLS se soporta solamente en el ESA.

Usted debe completar estos pasos del S A CLI para modificar las cifras SSL:

1. Salve el archivo de configuración S A a su computadora local.
2. Abra el archivo XML.
3. Busque para la sección del *<ssl>* en el 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. Modifique las cifras según lo deseado y salve el 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. Cargue el nuevo archivo de configuración sobre el S A.

6. **Someta** y **confíe** todos los cambios.

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De febrero el 19 de 2015
ID del Documento: 117864