9.5 y un AsyncOS más nuevo para la actualización de la seguridad del correo electrónico con una más vieja comunicación TLSv1.2 de los Certificados (MD5) a fallar

Contenido

Introducción

Este documento describe los pasos necesarios que se aplicarán si encuentra un problema con la comunicación de TLS, o accede la interfaz Web, después de actualizar a AsyncOS para la versión 9.5 posterior de la Seguridad del correo electrónico en los dispositivos de seguridad del correo electrónico de Cisco (ESA).

Los Certificados de la herencia (MD5) hacen la comunicación TLSv1.2 fallar en 9.5 AsyncOS para las actualizaciones de la seguridad del correo electrónico y más nuevo

> **Note**: Lo que sigue es una solución alternativa mencionada para los Certificados actuales de la versión parcial de programa aplicados en el dispositivo. Sin embargo, los pasos abajo pueden también dispositivo aplicarse a cualquier certificado firmado MD5.

Sobre todavía la ejecución de una actualización a AsyncOS para la versión 9.5 posterior de la Seguridad del correo electrónico, los Certificados uces de los de la versión parcial de programa de IronPort de la herencia funcionando y aplicados para la salida, recepción o LDAP, pueden experimentar los errores mientras que intentan comunicar vía TLSv1/TLSv1.2 con algunos dominios. El error de TLS hará todo el entrante o sesiones de salida fallar.

Si los Certificados se aplican a la interfaz HTTPS, los buscadores Web modernos no podrán acceder la interfaz Web del dispositivo.

Los registros del correo deben parecer similares al siguiente ejemplo:

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
```

'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Este error es causado por el algoritmo de la firma aplicado al certificado más viejo que es MD5; sin embargo, los Certificados asociados al dispositivo/al navegador de conexión soportan solamente los algoritmos basados firma SHA. Aunque, los Certificados más viejos de la versión parcial de programa que tiene la firma MD5 sean en el dispositivo el mismo tiempo el nuevo certificado basado SHA de la versión parcial de programa el error antedicho se manifestará solamente si el certificado basado firma MD5 se aplica a las secciones especificadas (es decir recepción, salida, etc.)

Abajo está un ejemplo tirado del cli de un dispositivo que tenga ambos los Certificados más viejos MD5 además del nuevo certificado de la versión parcial de programa (nota: el certificado más nuevo (versión parcial de programa) debe ser más nuevo es el algoritmo SHA y tener una fecha de vencimiento más larga que los Certificados más viejos de la versión parcial de programa).:

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

Acciones correctivas

1. Navegue a la red (UI): **Red > Certificados**
2. Verifique que usted haga actualmente los Certificados más viejos instalar y también tenga el nuevo certificado de la versión parcial de programa SHA.
3. De acuerdo con donde están aplicados los Certificados más viejos de la versión parcial de programa substituya esto por el nuevo certificado de la versión parcial de programa.

Estos Certificados se pueden encontrar típicamente el ser aplicado en las secciones siguientes:

- **Red > módulos de escucha > entonces nombre del módulo de escucha > del certificado**
- **El correo limpia > los controles del destino > edita las configuraciones globales > el certificado**
- **La red > la interfaz IP > eligen la interfaz asociada al acceso a GUI > al certificado HTTPS**
- **La administración del sistema > el LDAP > editan las configuraciones > el certificado**

4. Una vez que se han substituido todos los Certificados verifique de la línea de comando que la comunicación de TLS sea acertada ahora.

Ejemplo de trabajar la comunicación de TLS que es negociada usando 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
```

Acciones correctivas CLI (si el GUI no puede ser accedido)

El certificado puede necesitar ser modificado en cada interfaz IP que tenga un certificado habilitado para el servicio HTTPS. Para modificar el certificado funcionando para las interfaces, funcione con por favor los siguientes comandos en el CLI:

1. Teclee el **interfaceconfig**.
2. Select **edita**.
3. Ingrese el número de la interfaz que usted desea editar.
4. Utilice la tecla Retorno para validar las configuraciones actuales para cada pregunta presentada. Cuando la opción para que el certificado se aplique se presenta, seleccione el

certificado de la versión parcial de programa:

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. Acabe de caminar con los prompts de las configuraciones hasta que se completen todas las preguntas sobre configuración.
6. Utilice la tecla Retorno para salir al prompt principal CLI.
7. Usecommit para salvar sus cambios a la configuración.

Note: Recuerde por favor **confiar los** cambios después de cambiar el certificado funcionando en la interfaz.

Información Relacionada

- Guía completa de la configuración para TLS en el ESA
- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Dispositivo de la Administración del Cisco Security - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems