Errores de la conexión SGC: Eleve y exporte publicaciones del uso de las cifras diversas

Contenido

Introducción

Este documento aborda un problema que ocurra en el archivo del proveedor de seguridad Schannel.dll, que se utiliza en Microsoft Internet Information Server (IIS) y Microsoft Internet Explorer. Este problema presenta cuando usted conecta con un sitio que las aplicaciones Server Gated Cryptography (SGC) de hacer la encripción alta, y las aplicaciones de la habitación de la cifra de la exportación un algoritmo de troceo mientras que el conjunto cipher local utiliza otro. En esta situación, el archivo Schannel.dll selecciona de vez en cuando el algoritmo incorrecto, que da lugar a una falla de conexión. Como consecuencia, los clientes de Web pueden no poder conectar con los sitios web que utilizan el SGC para la encripción fuerte cuando se requiere una conexión segura. Si el servidor de Internet o el cliente de Web está funcionando con los productos Microsoft, después la conexión puede fallar.

Microsoft reconoce que cuando una cifra elevadora utiliza una diversa publicación que la cifra de la exportación, la conexión puede fallar. Para más información sobre este problema, refiera a las conexiones SGC puede fallar de los clientes nacionales .

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Cisco Content Services (CSS) con el módulo del Secure Socket Layer (SSL)

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.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Problema

Con un CERT elevador del SGC en el módulo CSS SSL, cuando el cliente conecta con un sitio a través del módulo SSL con un navegador 56-bit, el navegador establece una conexión SSL en 56 bastante que intensificando la conexión al 128.

Por ejemplo, imagínese que el primer saludo del cliente negocia una cifra del rsa-export1024-with-rc4-56-sha. Las coincidencias del módulo basadas en la orden en la configuración (a menos que se cargan las cifras) tan cuando ocurre el elevador, el módulo intentan probablemente utilizar una cifra de rsa-with-3des-ede-cbc-sha. Las publicaciones de estas dos cifras no hacen juego, y el error ocurre. No sólo deben las publicaciones hacer juego, PERO los tipos de encripción deben hacer juego también.

Solución

De acuerdo con la lista del proxy del cliente del ejemplo, las soluciones a este problema se explican en esta sección.

Actualmente, el cliente tiene estas cifras de la exportación:

- servidor del SSL 4
- direccionamiento 198.22.10.10 vip del servidor del SSL 4
- rsakey CSSRsaKey4 del servidor del SSL 4
- rsacert RsaCert4 del servidor del SSL 4
- cifra rsa-with-rc4-128-md5 198.22.10.10 20094 del servidor del SSL 4
- cifra rsa-with-rc4-128-sha 198.22.10.10 20094 del servidor del SSL 4
- rsa-with-des-cbc-sha 198.22.10.10 20094 de la cifra del servidor del SSL 4
- cifra rsa-with-3des-ede-cbc-sha 198.22.10.10 20094 del servidor del SSL 4
- cifra rsa-export1024-with-des-cbc-sha 198.22.10.10 20094 del servidor del SSL 4
- rsa-export1024-with-rc4-56-sha 198.22.10.10 20094 de la cifra del servidor del SSL 4

Para solucionar el problema discutido en este documento, usted debe escoger una cifra de la exportación para soportar (por ejemplo, rsa-export1024-with-rc4-56-sha). Esto no es generalmente un problema porque si un navegador 56-bit envía una de estas cifras, se envían ambos. Usted puede ahora configurar el resto de sus cifras fuertes, pero usted debe cargarlas tales que la cifra (rsa-with-rc4-128-sha) tiene la ponderación más alta. Las otras cifras fuertes se deben asignar las ponderaciones más fuertes siguientes, y la cifra de la exportación la

ponderación más baja. Aquí está una muestra de lo que parece esta configuración (nota que la cifra de la exportación no tiene ninguna ponderación pues el valor por defecto es 1):

Nota: En este ejemplo, usted tiene dos opciones en relación con las cuales habitación de la cifra de la exportación a utilizar. Cisco no puede recomendar cuál para utilizar. Usted debe tomar una decisión basada en sus requerimientos de seguridad del negocio.

Solución 1

Si usted decide utilizar la cifra de la exportación (rsa-export1024-with-rc4-56-sha), la lista del proxy parece esto:

- ponderación 10 de la cifra rsa-with-rc4-128-sha 198.22.124.134 20094 del servidor del SSL 5
- ponderación 8 de la cifra rsa-with-rc4-128-md5 198.22.124.134 20094 del servidor del SSL 5
- ponderación 8 de 198.22.124.134 20094 del rsa-with-des-cbc-sha de la cifra del servidor del SSL 5
- ponderación 8 de la cifra rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 del servidor del SSL 5
- ponderación 1 de 198.22.124.134 20094 del rsa-export1024-with-rc4-56-sha de la cifra del servidor del SSL 5

Solución 2

Si usted decide soportar la otra cifra de la exportación (rsa-export1024-with-des-cbc-sha), sus ponderaciones parecen esto:

- ponderación 10 de 198.22.124.134 20094 del rsa-with-des-cbc-sha de la cifra del servidor del SSL 5
- ponderación 8 de la cifra rsa-with-rc4-128-sha 198.22.124.134 20094 del servidor del SSL 5
- ponderación 8 de la cifra rsa-with-rc4-128-md5 198.22.124.134 20094 del servidor del SSL 5
- ponderación 8 de la cifra rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 del servidor del SSL 5
- ponderación 1 de la cifra rsa-export1024-with-des-cbc-sha 198.22.124.134 20094 del servidor del SSL 5

Información Relacionada

- Configurar el tráfico SSL con el CSS
- Soporte Técnico - Cisco Systems