Contenido

Introducción

Este documento describe los escenarios en los cuales Cisco unificó el cargamento de centro de la parada de las páginas web de la inteligencia (CUIC) en el internet explorer (IE) después de las actualizaciones del Knowledge Base de la instalación de Microsoft (KB).

El artículo también ofrece las soluciones alternativas/las soluciones potenciales de la perspectiva CUIC.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento en estos temas:

- La administración de Windows
- La administración y configuración CUIC

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco unificó el centro de la inteligencia 10.5(1)
- Cisco unificó la inteligencia 10.x de centro
- Cisco unificó el centro de la inteligencia 9.1(x)
- Windows 7 o 8
- Internet Explorer 11

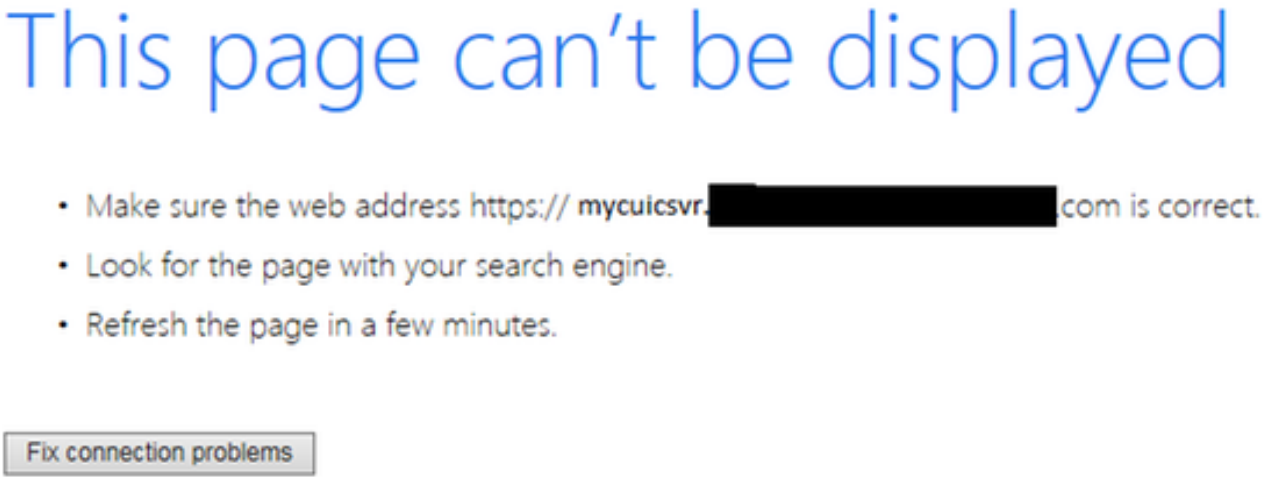
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de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

Situación

- Versión 9.1(1) CUIC o versión 10.5(1) CUIC

- Internet explorer (IE) 11 en Windows 7 o Windows 8
- Instale KB3161639 en Windows 7/8
- Link del lanzamiento CUIC en el Internet Explorer - DIRECCIÓN DE HOST *>/cuic de* http://<CUIC

Esto indica con el mensaje de error tal y como se muestra en de la imagen:



¿?

Análisis

Microsoft agregó las nuevas habitaciones de la cifra, tal y como se muestra en de la imagen, como parte de rollup KB3161608 de la actualización de de junio de 2016.

Cipher suite	FIPS mode enabled	Protocols	Exchange	Encryption	Hash
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes	TLS 1.2, TLS 1.1, TLS 1.0	DHE	AES	SHA1

¿?

Como parte de KB3161639, **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** y **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** se agregan a las habitaciones de la cifra y la pedido de la prioridad predeterminada de las habitaciones de la cifra se cambia en el OS (Sistema operativo) Windows.

Debido a esto si las máquinas del cliente tienen las actualizaciones antedichas, tienden a comunicar usando **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** con el servidor del tomcat CUIC (mientras que **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** se define en sus config del conector del tomcat CUIC).

Sin embargo, la comunicación usando la cifra **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** no trabaja. Esto está debido al requerimiento mínimo de 1024 bits para las claves del intercambio del Diffie Hellman (DHE) aplicadas por Microsoft para reparar el ataque del amontonamiento.

CUIC hasta que la versión 11.x tenga la Java 6 versiones que soporta solamente 768 claves del bit. Así, puede causar un error del apretón de manos.

Solución

Éste es no corresponde a CUIC 11.0(1) donde se resuelve este problema. Para las versiones CUIC 9.1(1) y las versiones 10.x, esto es resuelto por el archivo abierto del POLI SSL disponible aquí

Como parte del poli del openssl, el soporte de la cifra de Diffie Hellman (DHE) es quitado del conector del tomcat CUIC quitando **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** para prevenir el ataque del amontonamiento.