Contenu

Introduction

Ce document décrit les scénarios dans lesquels les pages Web du centre d'intelligence de Cisco Unified (CUIC) cessent de charger sur l'Internet Explorer (IE) après l'installation des mises à jour de base de connaissances de Microsoft (KO).

L'article offre également des contournements/solutions potentiels du point de vue du CUIC.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance sur ces thèmes :

- Gestion de Windows
- Gestion et configuration CUIC

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Centre d'intelligence de Cisco Unified 10.5(1)
- Centre 10.x d'intelligence de Cisco Unified
- Centre d'intelligence de Cisco Unified 9.1(x)
- Windows 7 ou 8
- Internet Explorer 11

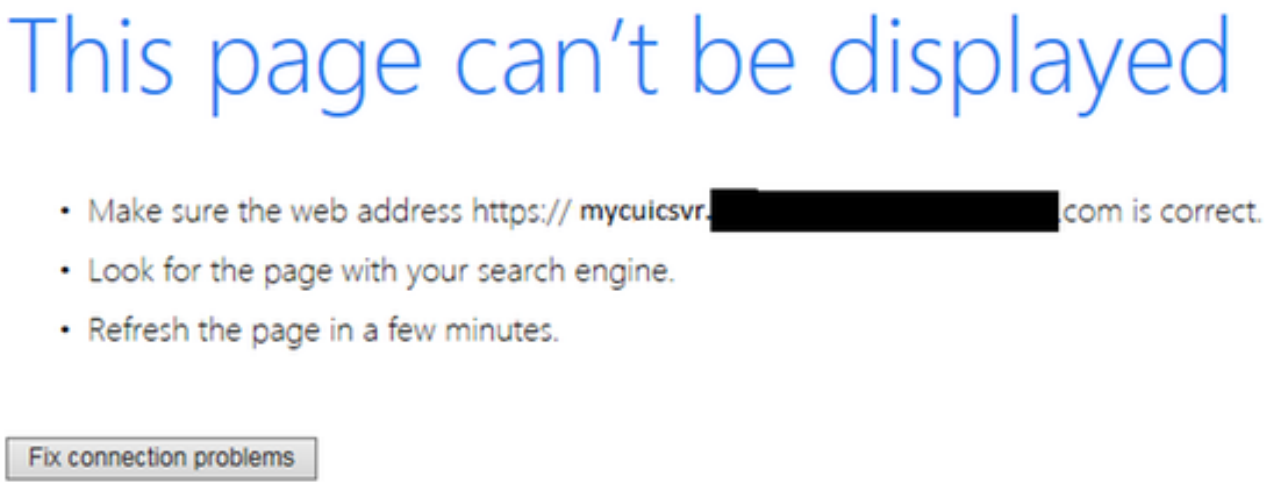
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez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

Scénario

- Version 9.1(1) CUIC ou version 10.5(1) CUIC
- Internet Explorer (IE) 11 sur le Windows 7 ou le Windows 8

- Installez KB3161639 sur Windows 7/8
- Lien du lancement CUIC sur l'Internet Explorer - HOST ADDRESS >/*cuic de* http:// <CUIC

Ceci incite avec le message d'erreur suivant les indications de l'image :



?

Analyse

Microsoft a ajouté les nouvelles suites de chiffrement, suivant les indications de l'image, comme partie de la remontée pyramidale KB3161608 de mise à jour de juin 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

?

En tant qu'élément de KB3161639, **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** et **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** sont ajoutés aux suites de chiffrement et la commande prioritaire par défaut des suites de chiffrement sont changées dans le système d'exploitation windows.

Pour cette raison si les machines cliente ont les mises à jour ci-dessus, elles tendent à communiquer utilisant **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** avec le serveur de chat CUIC (pendant que **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** est défini dans son config de connecteur de chat CUIC).

Cependant, la transmission utilisant le chiffrement **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** ne fonctionne pas. C'est en raison de la condition requise minimum de 1024 bits pour les clés de l'échange de Diffie Hellman (DHE) imposées par Microsoft pour réparer l'attaque d'embouteillage.

CUIC jusqu'à ce que la version 11.x ait Java 6 versions qui prend en charge seulement 768 clés de bit. Ainsi, il peut entraîner une panne de prise de contact.

Solution

Ce s'applique pas applicable à CUIC 11.0(1) où cette question est résolue. Pour des versions de versions 9.1(1) et 10.x CUIC, ceci est résolu par le fichier ouvert de COP SSL disponible ici

En tant qu'élément du cop d'openssl, le support de chiffrement de Diffie-Hellman (DHE) est enlevé du connecteur de chat CUIC en retirant **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** pour empêcher l'attaque d'embouteillage.