Les pages UCCX 10.6 ne charge pas dans IE11 après l'installation de Microsoft KB3161608/KB3161606

Contenu

Introduction

Ce document décrit les scénarios qui peuvent avoir comme conséquence les pages Web du Cisco Unified Contact Center Express (UCCX) et/ou de la finesse ne chargeant pas, selon lesquelles la version d'UCCX 10.6 est installée.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestion de Windows
- Gestion et configuration UCCX

Composants utilisés

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

- Cisco Unified Contact Center Express 10.6(1)
- Cisco Unified Contact Center Express 10.6(1) SU1
- Windows 7 ou 8
- Internet Explorer 11

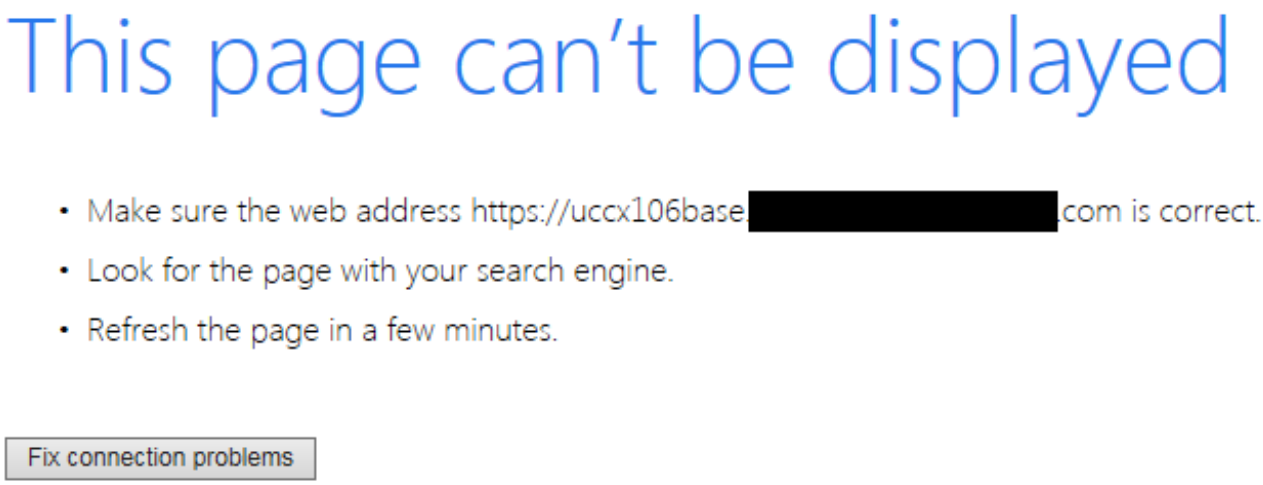
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez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

Scénario 1

- Version de base UCCX 10.6(1) avec le Secure Hash Algorithm (certificat SHA)1 ou SHA256
- Internet Explorer (IE) 11 pour le Windows 7 ou 8
- Installez KB3161608 sur le Windows 7 ou KB3161606 sur Windows 8

Résultat

Quand vous naviguez vers la page de connexion d'admin ou de finesse de Web UCCX dans les résultats IE11 dans ce message étant affiché « cette page ne peut pas être affichée ».



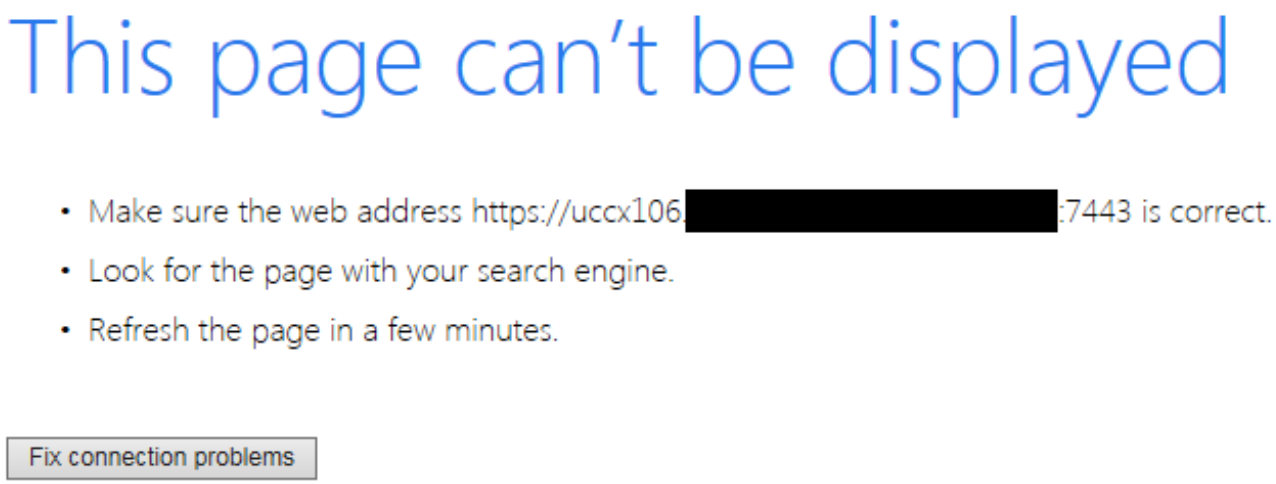
Scénario 2

- UCCX 10.6(1) SU1 avec certificat SHA1 ou SHA256
- IE11 pour le Windows 7 ou 8
- Installez KB3161608 sur le Windows 7 ou KB3161606 sur Windows 8

Résultat

Ce scénario résulte dans ceci :

- La page d'admin de Web UCCX obtient chargé et te permet pour ouvrir une session avec succès.
- La page de connexion de finesse obtient chargé et permet à l'utilisateur pour entrer dans les qualifications. Cependant, la finesse incite l'utilisateur à recevoir les 7443 Certificats mais la page ne charge pas avec le même message - « cette page ne peut pas être affichée ».



Analyse

Les KBs sont réellement un paquet de mises à jour qui installe cette un en particulier **mise à jour KB3161639 pour ajouter de nouvelles suites de chiffrement à l'Internet Explorer et à la périphérie de Microsoft dans Windows**. Pendant que vous regardez plus étroitement ce KO, ces suites de chiffrement de deux Transports Layer Security (TLS) sont ajoutées à la liste de ceux utilisée par l'IE : TLS_DHE_RSA_WITH_AES_128_CBC_SHA et TLS_DHE_RSA_WITH_AES_256_CBC_SHA.

Dans Firefox ceux-ci peuvent être désactivés par cette procédure :

1. Naviguez vers environ : config.
2. Recherchez **security.ssl3.dhe** dans cela.
3. Double-cliquer sur **security.ssl3.dhe_rsa_aes_256_sha** et **security.ssl3.dhe_rsa_aes_128_sha** pour les placer à faux.

Cependant avec IE11 il y a aucun contournement qui ne peut être fait par le navigateur. Au lieu de cela, un administrateur modifie la stratégie de groupe de gens du pays ou de domaine pour exclure les chiffrements dans la configuration SSL.

Afin de modifier la stratégie locale par le module **gpedit.msc Windows**, naviguez vers la **commande >Administrative de suite de chiffrement des paramètres de configuration >SSL du >Network >SSL d'outils de** ComputerConfiguration**.**

Si la commande de suite est placée **handicapée** ou puis **pas configurée l'**ordre par défaut est utilisé et l'accès de bloc à UCCX/Finesse. Au lieu de cela, ceci devrait être placé à **activer** et la commande de suite de chiffrement devrait être modifiée pour exclure les deux chiffrements mentionnés ci-dessus. Notez la restriction que la liste de chiffrements doivent être utilisées, car ils ne peuvent pas dépasser 1023 caractères de longueur. La liste de chiffrement connue pour fonctionner avec UCCX/Finesse 10.6 est en tant que ces derniers :

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
```

L'autre option est de retirer KB3161608 ou KB3161606 de tous les ordinateurs qui doivent accéder à l'admin de finesse ou de Web UCCX.

Cette question ne présente pas dans UCCX 10.6(1) SU2 ou 11.0 comme la vulnérabilité d'embouteillage a été réparée dans ces versions. Il y a un défaut associé avec cette question, CSCuv89545, qui est résolu dans UCCX 10.6 SU1 ES02 et SU2. Un défaut relatif, CSCuu82538, est résolu dans des virtual machine exécutant le Red Hat Entreprise 6 comme SYSTÈME D'EXPLOITATION d'invité.

> Remarque: Une mise à jour semblable pour Windows 10 (KB3163018) fait également produire cette question dans les versions 10.6 et 10.6 SU1 UCCX en utilisant IE11. Cependant, Windows 10 n'est pas un système d'exploitation pris en charge pour ces versions d'UCCX et ne devrait pas être utilisé. Quand Windows 10 est utilisé, la question peut être résolue si vous utilisez Firefox, améliorez UCCX à la version 10.6 SU2 ou retirez la mise à jour de KO