Échecs de la connexion SGC : Les chiffrements Step-up et Export utilisent différents digests

Contenu

Introduction

Ce document aborde un problème qui se pose dans le fichier du fournisseur Schannel.dll de Sécurité, qui est utilisé dans Microsoft Internet Information Server (IIS) et Microsoft Internet Explorer. Ce problème présente quand vous vous connectez à un site qui emploie le chiffrement déclenché par serveur (SGC) pour faire le cryptage élevé, et la suite de chiffrement d'exportation utilise un algorithme de hachage tandis que la suite domestique de chiffrement utilise des autres. Dans cette situation, le fichier Schannel.dll sélectionne de temps en temps l'algorithme faux, qui a comme conséquence une connexion défectueuse. En conséquence, les clients web peuvent pour se connecter aux sites Web qui utilisent SGC pour le cryptage fort quand une connexion sécurisée est exigée. Si le serveur Internet ou le client web exécute des Produits de Microsoft, alors la connexion peut échouer.

Microsoft reconnaît que quand un chiffrement survolteur utilise un condensé différent que le chiffrement d'exportation, la connexion peut échouer. Pour plus d'informations sur ce problème, référez-vous aux connexions SGC peut échouer des clients domestiques .

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Services de contenu de Cisco (CSS) avec le module de Protocole SSL (Secure Socket Layer)

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.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Problème

Avec un SGC avancez le CERT sur le module SSL CSS, quand le client se connecte à un site par le module SSL à un navigateur 56-bit, le navigateur établit une connexion SSL à 56 plutôt qu'en intensifiant la connexion à 128.

Par exemple, imaginez que le premier client bonjour négocie un chiffrement de rsa-export1024-with-rc4-56-sha. Les correspondances de module basées sur la commande dans la configuration (à moins que les chiffrements sont pesés) ainsi quand le survolteur se produit, de module les essais probablement pour utiliser un chiffrement de rsa-with-3des-ede-cbc-sha. Les condensés de ces deux chiffrements ne s'assortissent pas, et la panne se produit. Non seulement doivent les condensés s'assortir, MAIS les types de cryptage doivent s'assortir aussi bien.

Solutions

Basé sur la liste de proxy de client d'exemple, la solution au problème sont expliquées dans cette section.

Actuellement, le client a ces chiffrements d'exportation :

- SSL-serveur 4
- adresse 198.22.10.10 de VIP du SSL-serveur 4
- rsakey CSSRsaKey4 du SSL-serveur 4
- rsacert RsaCert4 du SSL-serveur 4
- chiffrement rsa-with-rc4-128-md5 198.22.10.10 20094 du SSL-serveur 4
- chiffrement rsa-with-rc4-128-sha 198.22.10.10 20094 du SSL-serveur 4
- RSA-avec-DES-cbc-SHA 198.22.10.10 20094 de chiffrement du SSL-serveur 4
- chiffrement rsa-with-3des-ede-cbc-sha 198.22.10.10 20094 du SSL-serveur 4
- chiffrement rsa-export1024-with-des-cbc-sha 198.22.10.10 20094 du SSL-serveur 4
- chiffrement rsa-export1024-with-rc4-56-sha 198.22.10.10 20094 du SSL-serveur 4

Pour résoudre le problème discuté dans ce document, vous devez sélectionner un chiffrement d'exportation pour prendre en charge (par exemple, rsa-export1024-with-rc4-56-sha). Ce n'est habituellement pas un problème parce que si un navigateur 56-bit envoie un de ces chiffrements, chacun des deux sont envoyés. Vous pouvez maintenant configurer le reste de vos chiffrements forts, mais vous devez les peser tels que le chiffrement (rsa-with-rc4-128-sha) a le poids le plus élevé. Les autres chiffrements forts doivent être assignés les prochains poids les plus forts, et le

chiffrement d'exportation le plus bas poids. Voici un échantillon de ce que ressemble à cette configuration (la note que le chiffrement d'exportation n'a aucun poids car le par défaut est 1) :

Remarque: Dans cet exemple, vous avez deux options concernant lesquelles suite de chiffrement d'exportation à l'utiliser. Cisco ne peut pas recommander lesquels pour l'utiliser. Vous devez faire une décision fondée sur vos exigences de sécurité d'affaires.

Solution 1

Si vous décidez d'utiliser le chiffrement d'exportation (rsa-export1024-with-rc4-56-sha), la liste de proxy ressemble à ceci :

- poids 10 du chiffrement rsa-with-rc4-128-sha 198.22.124.134 20094 du SSL-serveur 5
- poids 8 du chiffrement rsa-with-rc4-128-md5 198.22.124.134 20094 du SSL-serveur 5
- poids 8 de 198.22.124.134 20094 de RSA-avec-DES-cbc-SHA de chiffrement du SSL-serveur 5
- poids 8 du chiffrement rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 du SSL-serveur 5
- poids 1 du chiffrement rsa-export1024-with-rc4-56-sha 198.22.124.134 20094 du SSL-serveur 5

Solution 2

Si vous décidez de prendre en charge l'autre chiffrement d'exportation (rsa-export1024-with-des-cbc-sha), vos poids ressemblent à ceci :

- poids 10 de 198.22.124.134 20094 de RSA-avec-DES-cbc-SHA de chiffrement du SSL-serveur 5
- poids 8 du chiffrement rsa-with-rc4-128-sha 198.22.124.134 20094 du SSL-serveur 5
- poids 8 du chiffrement rsa-with-rc4-128-md5 198.22.124.134 20094 du SSL-serveur 5
- poids 8 du chiffrement rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 du SSL-serveur 5
- poids 1 du chiffrement rsa-export1024-with-des-cbc-sha 198.22.124.134 20094 du SSL-serveur 5

Informations connexes

- Configurer le trafic SSL par le CSS
- Support technique - Cisco Systems