IM et présence et questions et réponses de certificat ECDSA

Contenu

Introduction

Ce document répond à des questions liées aux Certificats elliptiques de l'algorithme de signature numérique de curve (ECDSA) qui fonctionne avec Cisco IM et la présence (appliance IM&P).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager (CUCM)

- Cisco IM et présence (PIM)
- Protocole SIP (Session Initiation Protocol)
- Couplage de la téléphonie et de l'informatique (CTI)
- Cryptage de Rivest-Shamir-Adleman (RSA)
- Algorithme elliptique de signature numérique de curve (ECDSA)
- Messagerie et présence extensibles Protocol (XMPP)

Composants utilisés

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

- Cisco IM et présence 11.5.1

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Discussion d'équipe de produit IM&P sur ECDSA

En référence aux chiffrements de Transport Layer Security de paramètre d'entreprise (TLS), la sélection par défaut est **tous les chiffrements RSA préférés**. Ainsi en référence au paramètre le TLS chiffre, les questions suivantes a été augmenté avec l'équipe technique IM&P.

> Remarque: Toutes les questions sont répondues et vérifiées par l'équipe technique IM&P.

Fait-il ce paramètre dit-il les sélections RSA IM&P s'il doit choisir entre la RSA et l'ECDSA ?

Oui. Ce paramètre est seulement pour l'interface CUCM SIP/CTI. Des chiffrements RSA est donnés la préférence au-dessus d'ECDSA.

Dans quelles conditions Cisco IM et la présence peuvent-ils envoyer ECDSA quoique tous les chiffrements RSA Preferred soit sélectionnés ?

Il est pour donner la préférence aux chiffrements RSA mais il a des chiffrements ECDSA aussi bien, mais quand le client initie une connexion il envoie des chiffrements RSA au-dessus d'ECDSA.

Si ECDSA a la haute priorité, peut-il être choisi quoique tous les chiffrements RSA Preferred soit sélectionnés ?

Oui. Ce paramètre entre dans l'image seulement quand CUCM agit en tant que client. La

préférence est donnée pour passer commande dans ce que le client initie la connexion. Si le client initie une connexion avec ECDSA chiffre sur le dessus, alors la connexion se produit avec ECDSA. Sinon alors alors la RSA est donnée la préférence.

On peut évidemment sélectionner quels chiffrements a la haute priorité. Quand un client de tiers envoie un message Hello avec sa suite de chiffrement, Cisco IM et présence choisit le chiffrement le plus fort de cette liste sur le TLS fait-il chiffrent le mappage pour la page de clients de tiers que le serveur et le client prennent en charge ?

Oui. Quand le serveur agit en tant que client il envoie le chiffrement dans la commande on lui mentionne que dans les questions précédentes.

Y a-t-il un document qui clarifie ces choses ?

Oui. Il y a une option d'aide dès que vous sélectionnerez le **TLS que les chiffrements** joignent à la page de paramètres d'entreprise qui énonce la liste des chiffrements pris en charge.

Tous les chiffrements RSA ont préféré des sujets de paramètre seulement quand CUCM/IMP agit en tant que client ?

Oui.

Est-ce qu'il signifie-t-il que CUCM/IMP (client) envoie des Certificats RSA et ECDSA mais des Certificats RSA peut avoir plus prioritaire ?

Oui.

Sur le TLS chiffrez la page d'aide qu'elle indique que des chiffrements sont inclus dans cette commande. Fait-il ce moyen que des chiffrements sont introduits cette commande quand cette option est sélectionnée ?

Tous les chiffrements RSA préférés

Inclut des chiffrements dans l'ordre suivant :

TLS_ECDHE_RSA avec AES256_GCM_SHA384

TLS_ECDHE_ECDSA avec AES256_GCM_SHA384

TLS_ECDHE_RSA avec AES128_GCM_SHA256

TLS_ECDHE_ECDSA avec AES128_GCM_SHA256

TLS_RSA avec AES_128_CBC_SHA1

Oui.

Les tous les chiffrements RSA ont préféré le paramètre n'importe pas quand CUCM/IMP agit en tant que serveur. Le CUCM/IMP dans ce cas répond avec un type de certificat qui a le plus prioritaire dans le message Hello du client ?

Oui.

Si ce paramètre se réfère seulement à SIP/CTI, y a-t-il un paramètre équivalent pour des connexions de TLS avec des interfaces XMPP ?

Non. Il y a une amélioration de caractéristique pour XMPP, mais il n'est pas encore mis en application.