Fragen und Antworten zum IM- und Presence- und ECDSA-Zertifikat

Inhalt

Einführung

Dieses Dokument beantwortet Fragen zu ECDSA-Zertifikaten (Elliptic Curve Digital Signature Algorithm), die mit der Cisco IM and Presence (IM&P)-Appliance kompatibel sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM)
- Cisco IM und Presence (IMP)

- Session Initiation Protocol (SIP)
- Integration von Computertelefonie (CTI)
- Rivest-Shamir-Adleman (RSA)-Verschlüsselung
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Extensible Messaging and Presence Protocol (XMPP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IM und Presence 11.5.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

IM&P-Produktteam-Diskussion über ECDSA

In Bezug auf die TLS-Verschlüsselungen (Transport Layer Security) der Enterprise-Parameter ist die Standardauswahl **Alle Ciphers RSA Preferred (Alle Ciphers RSA Preferred)**. Im Hinblick auf Parameter-TLS-Chiffren wurden daher beim IM&P Engineering-Team die folgenden Fragen gestellt.

> **Hinweis**: Alle Fragen werden vom IM&P Engineering Team beantwortet und geprüft.

Weist dieser Parameter IM&P RSA aus, wenn er zwischen RSA und ECDSA wählen muss?

Ja. Dieser Parameter ist nur für CUCM-SIP/CTI-Schnittstellen vorgesehen. RSA-Chiffren wird gegenüber ECDSA bevorzugt.

Unter welchen Bedingungen kann Cisco IM und Presence ECDSA senden, obwohl All Ciphers RSA Preferred ausgewählt wurde?

Es soll RSA-Verschlüsselungen bevorzugt werden, aber es gibt auch ECDSA-Verschlüsselungen, aber wenn der Client eine Verbindung initiiert, sendet er RSA-Verschlüsselungen über ECDSA.

Wenn ECDSA eine höhere Priorität hat, kann diese ausgewählt werden, obwohl All Ciphers RSA Preferred (Alle Ciphers RSA-Priorität) ausgewählt wurde?

Ja. Dieser Parameter wird nur angezeigt, wenn CUCM als Client fungiert. Die Präferenz wird der

Reihenfolge zugewiesen, in der der Client die Verbindung initiiert. Wenn der Client oben eine Verbindung mit ECDSA-Chiffren herstellt, erfolgt die Verbindung mit ECDSA. Andernfalls wird RSA bevorzugt.

Man kann natürlich auswählen, welche Chiffren die höchste Priorität haben. Wenn ein Drittanbieter-Client mit seiner Verschlüsselungssuite eine Hello-Nachricht sendet, wählt Cisco IM und Presence auf der TLS Cipher Mapping-Seite für Drittanbieter-Clients den stärksten Chiffre aus dieser Liste aus, den der Server und der Client unterstützen?

Ja. Wenn der Server als Client agiert, sendet er die Chiffre in der Reihenfolge, in der sie in den vorherigen Fragen erwähnt wurde.

Gibt es ein Dokument, das diese Dinge erläutert?

Ja. Sobald Sie den Link **TLS Ciphers** auf der Seite für die Unternehmensparameter auswählen, wird eine Hilfeoption bereitgestellt, die die Liste der unterstützten Chiffren enthält.

Alle Ciphers RSA Preferred-Parameter sind nur wichtig, wenn CUCM/IMP als Client agiert?

Ja.

Bedeutet dies, dass CUCM/IMP (Client) RSA- und ECDSA-Zertifikate sendet, RSA-Zertifikate jedoch die höchste Priorität haben können?

Ja.

Auf der Hilfeseite für TLS-Chiffren wird angegeben, dass in dieser Bestellung Chiffren enthalten sind. Bedeutet das, dass Chiffren in dieser Reihenfolge gesendet werden, wenn diese Option aktiviert ist?

Alle Ciphers RSA Preferred

Schließt Ciphers in die folgende Reihenfolge ein:

TLS_ECDHE_RSA mit AES256_GCM_SHA384

TLS_ECDHE_ECDSA mit AES256_GCM_SHA384

TLS_ECDHE_RSA mit AES128_GCM_SHA256

TLS_ECDHE_ECDSA mit AES128_GCM_SHA256

TLS_RSA mit AES_128_CBC_SHA1

Ja.

Der Parameter All Ciphers RSA Preferred (Alle Ciphers RSA Preferred) spielt keine Rolle, wenn CUCM/IMP als Server fungiert. Der CUCM/IMP antwortet in diesem Fall mit einem Zertifikatstyp, der in der Hello-Nachricht des Clients die höchste Priorität hat?

Ja.

Wenn sich dieser Parameter nur auf SIP/CTI bezieht, gibt es einen entsprechenden Parameter für TLS-Verbindungen mit XMPP-Schnittstellen?

Nein. Es gibt eine Funktionsverbesserung für XMPP, die jedoch noch nicht implementiert ist.