Vragen en antwoorden met certificaten voor IM en Presence en ECDSA

Inhoud

Inleiding

Dit document beantwoordt vragen over de Elliptic Curve Digital Signature Algorithm (ECDSA)-certificaten die met het Cisco IM and Presence (IM&P)-apparaat werken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

- Session Initiation Protocol (SIP)
- Computer Telephony Integration (CTI)
- Rivest-Shamir-Adleman (RSA)-encryptie
- Ellips Curve Digital Signature Algorithm (ECDSA)
- Extensible Messaging and Presence Protocol (XMPP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IM and Presence 11.5.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

IM&P productteamdiscussie op ECDSA

Onder verwijzing naar de ondernemingsparameter Transport Layer Security (TLS)-ciphers, is de standaardselectie **Alle CIFERS RSA voorkeur**. Wat parameter TLS-ciphers betreft, werden de volgende vragen gesteld aan het IM&P-team.

> Opmerking: Alle vragen worden beantwoord en geverifieerd door het IM&P Engineering Team.

Heeft deze parameter IM&P een optie op RSA als deze moet kiezen tussen RSA en ECDSA?

Ja. Deze parameter is alleen voor CUCM SIP/CTI-interface. RSA-ciphers krijgen de voorkeur boven ECDSA.

Onder welke voorwaarden kan Cisco IM and Presence ECDSA verzenden zelfs al wordt de voorkeur gegeven aan Alle CIFERS RSA geselecteerd?

Het gaat om het geven van de voorkeur aan RSA-ciphers, maar het heeft ook ECDSA-ciphers, maar wanneer client een verbinding initieert, stuurt het RSA-ciphers boven ECDSA.

Als ECDSA een hogere prioriteit heeft, kan het worden gekozen zelfs alhoewel Alle Ciphers RSA Geprefereerd wordt geselecteerd?

Ja. Deze parameter komt alleen in het beeld als CUCM als client werkt. De voorkeur wordt gegeven aan order waarin de cliënt de verbinding initieert. Als de client een verbinding met

ECDSA-ciphers aan de bovenkant op gang brengt, dan gebeurt de verbinding met ECDSA. Als dit niet het geval is, krijgt RSA de voorkeur.

Je kunt duidelijk kiezen welke ciphers de hoogste prioriteit hebben. Wanneer een klant van een derde partij een Hallo bericht verstuurt met zijn zoekreeks, kiest Cisco IM and Presence het sterkste algoritme uit deze lijst in de TLS Cipher Mapping voor de pagina van de cliënten van de 3de partij die zowel de server als de cliënt steunt?

Ja. Wanneer een server als client handelt, stuurt hij het algoritme in de volgorde waarin het in de vorige vragen wordt genoemd.

Is er een document dat deze zaken verduidelijkt?

Ja. Er is een Help-optie zodra u de link **TLS-**cifen selecteert op de pagina met ondernemingsparameters, waarin de lijst staat van de ondersteunde ciphers.

Alle ciphers RSA voorkeurparameter is slechts van belang wanneer CUCM/IMP als cliënt handelt?

Ja.

Betekent dit dat CUCM/IMP (cliënt) zowel RSA- als ECDSA-certificaten stuurt, maar dat RSA-certificaten de hoogste prioriteit kunnen hebben?

Ja.

Op de Help-pagina van het TLS-algoritme staat dat cifen in deze volgorde zijn opgenomen. Betekent dit dat ciphers in die volgorde worden verstuurd wanneer deze optie is geselecteerd?

Alle ciphers RSA voorkeur

Omvat ciferen in de volgende volgorde:

TLS_ECDHE_RSA met AES256_GCM_SHA384

TLS_ECDHE_ECDSA met AES256_GCM_SHA384

TLS_ECDHE_RSA met AES128_GCM_SHA256

TLS_ECDHE_ECDSA met AES128_GCM_SHA256

TLS_RSA met AES_128_CBC_SHA1

Ja.

De voorkeurparameter van alle CIFERS RSA maakt niet uit wanneer CUCM/IMP als server werkt. In dat geval reageert de CUCM/IMP met een certificaattype dat de hoogste prioriteit heeft in het bericht "Hallo" van de klant?

Ja.

Als deze parameter alleen naar SIP/CTI verwijst, is er een equivalente parameter voor TLS verbindingen met XMPP interfaces?

Nee. Er is een functieverbetering voor XMPP, maar deze wordt nog niet geïmplementeerd.