Perguntas e Respostas sobre IM e Presença e certificado ECDSA

Contents

Introduction

Este documento responde perguntas relacionadas aos certificados ECDSA (Elliptic Curve Digital Signature Algorithm) que funcionam com o dispositivo Cisco IM and Presence (IM&P).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM)
- Mensagens instantâneas e presença da Cisco (IMP)

- Protocolo de Iniciação da Sessão (SIP)
- Integração entre telefonia e computador (CTI)
- Criptografia Rivest-Shamir-Adleman (RSA)
- Algoritmo de assinatura digital de curva elíptica (ECDSA)
- eXtensible Messaging and Presence Protocol (XMPP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Mensagens instantâneas e presença da Cisco 11.5.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Discussão da equipe de produtos IM&P em ECDSA

Em referência ao parâmetro empresarial Transport Layer Security (TLS) ciphers, a seleção padrão é **All Ciphers RSA Preferred**. Então, em referência aos parâmetros de cifras TLS, as perguntas a seguir foram levantadas com a equipe de Engenharia IM&P.

> **Note**: Todas as perguntas são respondidas e verificadas pela equipe de engenharia IM&P.

Esse parâmetro diz que o IM&P escolhe o RSA se tiver que escolher entre RSA e ECDSA?

Yes. Esse parâmetro é somente para a interface SIP/CTI do CUCM. Os cifras RSA têm preferência sobre ECDSA.

Em que condições o Cisco IM and Presence pode enviar ECDSA mesmo que All Ciphers RSA Preferred esteja selecionado?

Épara dar preferência a cifras RSA, mas também tem cifras ECDSA, mas quando o cliente inicia uma conexão, ele envia cifras RSA acima de ECDSA.

Se o ECDSA tiver prioridade mais alta, ele pode ser escolhido mesmo que All Ciphers RSA Preferred esteja selecionado?

Yes. Esse parâmetro entra na imagem somente quando o CUCM atua como um cliente. A preferência é dada para a ordem em que o cliente inicia a conexão. Se o cliente iniciar uma conexão com cifras ECDSA na parte superior, então a conexão acontece com ECDSA. Caso contrário, a RSA recebe preferência.

Épossível, obviamente, selecionar quais cifras têm a prioridade

máxima. Quando um cliente terceirizado envia uma mensagem Hello com seu conjunto de cifras, o Cisco IM e Presence escolhe a cifra mais forte dessa lista na página Mapeamento de cifras TLS para clientes terceirizados que o servidor e o cliente suportam?

Yes. Quando o servidor atua como um cliente, ele envia a cifra na ordem em que é mencionado nas perguntas anteriores.

Há algum documento que esclareça essas coisas?

Yes. Há uma opção de ajuda assim que você seleciona o link **TLS Ciphers** na página de parâmetros da empresa que indica a lista das cifras suportadas.

O parâmetro RSA Preferred de todos os clientes só importa quando o CUCM/IMP está atuando como um cliente?

Yes.

Significa que o CUCM/IMP (cliente) envia certificados RSA e ECDSA, mas os certificados RSA podem ter a maior prioridade?

Yes.

Na página de ajuda da cifra TLS, diz-se que as cifras estão incluídas neste pedido. Isso significa que cifras são enviadas nessa ordem quando essa opção é selecionada?

Todos os clientes preferidos pelo RSA

Inclui Ciphers na seguinte ordem:

TLS_ECDHE_RSA com AES256_GCM_SHA384

TLS_ECDHE_ECDSA com AES256_GCM_SHA384

TLS_ECDHE_RSA com AES128_GCM_SHA256

TLS_ECDHE_ECDSA com AES128_GCM_SHA256

TLS_RSA com AES_128_CBC_SHA1

Yes.

O parâmetro RSA Preferred de All Ciphers não importa quando o CUCM/IMP atua como um servidor. Nesse caso, o CUCM/IMP responde com um tipo de certificado que tem a prioridade mais alta na mensagem Hello do cliente?

Yes.

Se esse parâmetro se refere somente ao SIP/CTI, há um parâmetro equivalente para conexões TLS com interfaces XMPP?

Não. Há uma melhoria de recurso para XMPP, mas ele ainda não foi implementado.