IM e presença e perguntas e resposta do certificado ECDSA

Índice

Introdução

Este documento responde às perguntas relativas aos Certificados elípticos do Digital Signature Algorithm da curva (ECDSA) que trabalha com Cisco IM e presença (dispositivo IM&P).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gerente das comunicações unificadas de Cisco (CUCM)
- Cisco IM e presença (IMP)

- Session Initiation Protocol (SIP)
- Integração de telefonia e computador (CTI)
- Criptografia de Rivest-Shamir-Adleman (RSA)
- Digital Signature Algorithm elíptico da curva (ECDSA)
- Protocolo elástico da Mensagem e da presença (XMPP)

Componentes Utilizados

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

- Cisco IM e presença 11.5.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Discussão da equipe do produto IM&P em ECDSA

Na referência às cifras do Transport Layer Security do parâmetro empresarial (TLS), a seleção do padrão é **todas as cifras RSA preferidas**. Assim na referência ao parâmetro o TLS calcula, as seguintes perguntas foi aumentado com o equipe de engenharia IM&P.

> Nota: Todas as perguntas são respondidas e verificadas pelo equipe de engenharia IM&P.

Faz este parâmetro diz as picaretas RSA IM&P se tem que escolher entre o RSA e o ECDSA?

Sim. Este parâmetro é somente para a relação CUCM SIP/CTI. As cifras RSA são dadas a preferência sobre ECDSA.

Sob que circunstâncias podem Cisco IM e a presença enviar ECDSA mesmo que todas as cifras RSA Preferred sejam selecionadas?

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

Se ECDSA tem a prioridade mais alta, pode ser escolhido mesmo que todas as cifras RSA Preferred sejam selecionadas?

Sim. Este parâmetro entra a imagem somente quando CUCM atua como um cliente. A preferência é dada para pedir em qual o cliente inicia a conexão. Se o cliente inicia uma conexão com o ECDSA calcula na parte superior, a seguir a conexão acontece com ECDSA. Se não o RSA é dado então então a preferência.

Um pode obviamente selecionar que cifras têm a prioridade máxima. Quando um cliente da 3ª parte envia um mensagem Hello Messages com sua série da cifra, faz Cisco IM e presença escolhem a cifra a mais forte desta lista no mapeamento da cifra TLS para clientes da 3ª parte paginam que o server e o suporte ao cliente?

Sim. Quando o server atua como um cliente envia a cifra na ordem que se menciona nas perguntas anterior.

Há algum documento que esclarecer estas coisas?

Sim. Há uma opção de ajuda assim que você selecionar o link das **cifras TLS na** página dos parâmetros empresariais que indica a lista das cifras apoiadas.

Todas as cifras RSA preferiram matérias do parâmetro somente quando CUCM/IMP está atuando como um cliente?

Sim.

Significa que CUCM/IMP (cliente) envia Certificados RSA e ECDSA mas Certificados RSA pode ter a prioridade mais alta?

Sim.

Na página da ajuda da cifra TLS diz que as cifras estão incluídas nesta ordem. Faz esse meio que as cifras estão enviadas nessa ordem quando esta opção é selecionada?

Todas as cifras RSA preferidas

Inclui cifras no 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

Sim.

Todas as cifras RSA preferiram o parâmetro não importam quando CUCM/IMP atua como um server. O CUCM/IMP nesse caso responde com um tipo do certificado que tenha a prioridade mais alta no mensagem Hello Messages do cliente?

Sim.

Se este parâmetro refere somente SIP/CTI, há um parâmetro equivalente para conexões TLS com relações XMPP?

Não. Há um aprimoramento de recursos para XMPP, mas não é executado ainda.