IM y presencia y preguntas y respuestas del certificado ECDSA

Contenido

Introducción

Este documento contesta a las preguntas relacionadas con los Certificados elípticos del Digital Signature Algorithm de la curva (ECDSA) que trabaja con Cisco IM y la presencia (dispositivo IM&P).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM)

- Cisco IM y presencia (IMP)
- Session Initiation Protocol (SIP)
- Computer Telephony Integration (CTI)
- Cifrado del Rivest-Shamir-Adleman (RSA)
- Digital Signature Algorithm elíptico de la curva (ECDSA)
- Mensajería y protocolo extensibles de la presencia (XMPP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IM y presencia 11.5.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Discusión del equipo del producto IM&P sobre ECDSA

En referencia a las cifras de Transport Layer Security del parámetro Enterprise (TLS), la selección predeterminada es **todas las cifras RSA preferidas**. Tan en referencia al parámetro TLS cifra, las preguntas siguientes fue aumentado con el equipo de ingeniería IM&P.

> Nota: Todas las preguntas son contestadas y verificadas por el equipo de ingeniería IM&P.

¿Hace este parámetro dice las selecciones RSA IM&P si tiene que elegir entre el RSA y ECDSA?

Sí. Este parámetro está solamente para la interfaz CUCM SIP/CTI. Las cifras RSA se dan la preferencia sobre ECDSA.

¿Bajo qué condiciones pueden Cisco IM y la presencia enviar ECDSA aunque se seleccionan todas las cifras RSA Preferred?

Está para dar la preferencia a las cifras RSA pero tiene cifras ECDSA también, pero cuando el cliente inicia una conexión él envía las cifras RSA sobre ECDSA.

¿Si ECDSA tiene prioridad más alta, puede ser elegido aunque se seleccionan todas las cifras RSA Preferred?

Sí. Este parámetro entra en la imagen solamente cuando CUCM actúa como cliente. La preferencia se da para ordenar en cuál inicia el cliente la conexión. Si el cliente inicia una conexión con ECDSA cifra en el top, después la conexión sucede con ECDSA. Si no entonces entonces el RSA se da la preferencia.

Uno puede seleccionar obviamente qué cifras tienen la prioridad máxima. ¿Cuando un cliente de las de otras compañías envía un mensaje Hello Messages con su habitación de la cifra, hace Cisco IM y presencia elige la cifra más fuerte de esta lista en la asignación de la cifra de TLS para los clientes de las de otras compañías paginaron que el servidor y el soporte de cliente?

Sí. Cuando el servidor actúa como cliente envía la cifra en la orden que se menciona en las preguntas anteriores.

¿Hay documento que aclare estas cosas?

Sí. Hay una opción de ayuda tan pronto como usted seleccione el link de las **cifras de TLS** en la página de los parámetros Enterprise que estado la lista de las cifras soportadas.

¿Todas las cifras RSA prefirieron las materias del parámetro solamente cuando CUCM/IMP está actuando como cliente?

Sí.

¿Significa que CUCM/IMP (cliente) envía los Certificados RSA y ECDSA pero los Certificados RSA puede tener prioridad más alta?

Sí.

En la página de la ayuda de la cifra de TLS dice que las cifras están incluidas en esta orden. ¿Hace ese medio que las cifras están enviadas en esa orden cuando se selecciona esta opción?

Todas las cifras RSA preferidas

Incluye las cifras en el siguiente orden:

TLS_ECDHE_RSA con AES256_GCM_SHA384

TLS_ECDHE_ECDSA con AES256_GCM_SHA384

TLS_ECDHE_RSA con AES128_GCM_SHA256

TLS_ECDHE_ECDSA con AES128_GCM_SHA256

TLS_RSA con AES_128_CBC_SHA1

Sí.

Todas las cifras RSA prefirieron el parámetro no importan cuando CUCM/IMP actúa como servidor. ¿El CUCM/IMP en ese caso responde con un tipo de certificado que tenga la prioridad más alta en el mensaje Hello Messages del cliente?

Sí.

¿Si este parámetro se refiere solamente a SIP/CTI, hay un parámetro equivalente para las conexiones TLS con las interfaces XMPP?

No. Hay una mejora de las características para XMPP, pero todavía no se implementa.