أسئلة وإجابات حول المراسلة الفورية والحضور وشهادات ECDSA

المحتويات

المقدمة

يجيب هذا المستند على الأسئلة المتعلقة بشهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA) التي تعمل مع جهاز Cisco IM and Presence (IM&P).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- برنامج Cisco Unified Communications Manager (CUCM)
- المراسلة الفورية والحضور (IMP) من Cisco
- بروتوكول بدء جلسة عمل (SIP)
- دمج الاتصال الهاتفي بجهاز الكمبيوتر (CTI)

- تشفير Rivest-Shamir-Adleman (RSA)
- خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA)
- بروتوكول التواجد والمراسلة القابلة للتوسع (XMPP)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco IM and Presence 11.5.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

مناقشة فريق منتجات IM&P على ECDSA

في الإشارة إلى شرفات أمان طبقة نقل المعلمات (TLS) الخاصة بالمؤسسة، يكون التحديد الافتراضي هو **المفضل لـ All Ciphers RSA**. إذا بالإشارة إلى شرفة TLS للمعلمة، فإن الأسئلة التالية أثيرت مع فريق هندسة IM&P.

> **ملاحظة**: جميع الأسئلة يجيب عليها ويتحقق منها الفريق الهندسي التابع لشركة IM&P.

هل تعلم هذه المعلمة أن IM&P تختار RSA إذا كان يتعين عليها الاختيار بين RSA و ECDSA؟

نعم. هذه المعلمة خاصة بواجهة CUCM SIP/CTI فقط. تعطى تشفير RSA الأفضلية على ECDSA.

في أي ظروف يمكن أن يرسل Cisco IM و Presence ECDSA حتى ولو تم تحديد جميع التشفير الذي يفضله RSA؟

ويكون هذا إلعطاء الأفضلية لشرفات RSA ولكنه يحتوي على شرفات ECDSA أيضا، ولكن عندما يقوم العميل ببدء اتصال فإنه يرسل شرفات RSA فوق ECDSA.

إذا كان ECDSA لديه أولوية أعلى، هل يمكن إختياره حتى مع تحديد جميع التشفير المفضل RSA؟

نعم. ال تظهر هذه المعلمة في الصورة إلا عندما يعمل CUCM كعميل. تعطى الأفضلية للترتيب الذي يقوم العميل من خلاله بتهيئة الاتصال. إذا قام العميل ببدء اتصال بشرفات ECDSA في الأعلى، فيحدث الاتصال ب ECDSA. وإذا لم يكن الأمر كذلك، فيكون RSA هو الأفضلية.

يمكن للمرء بوضوح تحديد المشرفات التي لها الأولوية العليا. عندما يرسل عميل من جهة خارجية رسالة Hello مع

مجموعة التشفير الخاصة به، هل يقوم Cisco IM و Presence باختيار أقوى تشفير من هذه القائمة على تعيين تشفير TLS لصفحة عملاء الجهات الخارجية التي يدعمها الخادم والعميل؟

نعم. عندما يعمل الخادم كعميل فإنه يرسل التشفير بالترتيب المذكور في الأسئلة السابقة.

هل من وثيقة توضح هذه الأمور؟

نعم. هناك خيار تعليمات برمجي تحديد إرتباط **شفرات** TLS في صفحة معلمات المؤسسة التي تذكر قائمة الشفرات المدعومة.

هل تكون المعلمة المفضلة ل All Ciphers RSA مهمة فقط عندما يعمل CUCM/IMP كعميل؟

نعم.

هل يعني ذلك أن CUCM/IMP (العميل) يرسل شهادات RSA و ECDSA ولكن شهادات RSA يمكن أن تكون لها أعلى أولوية؟

نعم.

في صفحة تعليمات تشفير TLS، يتم تضمين المشفرات بهذا الترتيب. هل يعني ذلك أن المشفرات يتم إرسالها بهذا الترتيب عند تحديد هذا الخيار؟

جميع التشفير المفضل RSA

يتضمن الشفرات بالترتيب التالي:

TLS_ECDHE_RSA مع AES256_GCM_SHA384

TLS_ECDHE_ECDSA مع AES256_GCM_SHA384

TLS_ECDHE_RSA مع AES128_GCM_SHA256

TLS_ECDHE_ECDSA مع AES128_GCM_SHA256

TLS_RSA مع AES_128_CBC_SHA1

نعم.

المعلمة المفضلة RSA لكافة التشفير لا تهم عندما يعمل CUCM/IMP كخادم. يستجيب CUCM/IMP في هذه الحالة بنوع شهادة له أعلى أولوية في رسالة Hello الخاصة بالعميل؟

نعم.

إذا كانت هذه المعلمة تشير فقط إلى SIP/CTI، هل هناك معلمة مكافئة لاتصالات TLS بواجهات XMPP؟

لا. هناك تحسين لميزة XMPP، ولكنه لم يتم تنفيذه بعد.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).