Domande e risposte sui certificati per messaggistica immediata e presenza e ECDSA

Sommario

Introduzione

Questo documento risponde alle domande relative ai certificati ECDSA (Elliptic Curve Digital Signature Algorithm) compatibili con l'appliance Cisco IM e Presence (IM&P).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IM e Presence 11.5.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Discussione del team dei prodotti IM&P su ECDSA

In riferimento al parametro enterprise Transport Layer Security (TLS), la selezione predefinita è **All Ciphers RSA Preferred**. Quindi, in riferimento ai cifrari TLS, sono state poste le seguenti domande al team di IM&P Engineering.

> **Nota:** Tutte le domande ricevono risposta e vengono verificate dal team di progettazione di IM&P.

Questo parametro indica a IM&P di scegliere RSA se deve scegliere tra RSA e ECDSA?

Sì. Questo parametro è solo per l'interfaccia SIP/CTI CUCM. I cifrari RSA hanno la precedenza su ECDSA.

In quali condizioni Cisco IM e Presence possono inviare ECDSA anche se è stata selezionata l'opzione All Ciphers RSA Preferred (Tutti i dispositivi di crittografia RSA preferiti)?

Èper dare la preferenza ai cifrari RSA, ma ha anche cifrari ECDSA, ma quando il client avvia una connessione invia cifrari RSA sopra ECDSA.

Se ECDSA ha una priorità più alta, può essere scelto anche se è selezionata l'opzione Tutti i cifrari RSA preferiti?

Sì. Questo parametro viene visualizzato nell'immagine solo quando CUCM funge da client. La preferenza viene assegnata all'ordine in cui il client avvia la connessione. Se il client avvia una connessione con i cifrari ECDSA nella parte superiore, la connessione avviene con ECDSA. In

caso contrario, viene data la preferenza a RSA.

Naturalmente è possibile scegliere quali cifrari hanno la priorità principale. Quando un client di terze parti invia un messaggio Hello con la sua suite di cifratura, Cisco IM e Presence scelgono la cifratura più sicura da questo elenco nella pagina TLS Cipher Mapping for 3rd party Client che sia il server che il client supportano?

Sì. Quando il server funge da client, invia la cifratura nell'ordine indicato nelle domande precedenti.

C'è qualche documento che chiarisca queste cose?

Sì. Non appena si seleziona il collegamento **Cifre TLS** nella pagina dei parametri enterprise, è disponibile un'opzione di guida che indica la lista delle cifrature supportate.

Tutti i parametri Ciphers RSA Preferred sono rilevanti solo quando CUCM/IMP opera come client?

Sì.

Significa che CUCM/IMP (client) invia entrambi i certificati RSA ed ECDSA, ma i certificati RSA possono avere la massima priorità?

Sì.

Nella pagina di aiuto della cifratura TLS è indicato che i cifrari sono inclusi in questo ordine. Ciò significa che i cifrari vengono inviati in questo ordine quando questa opzione è selezionata?

Tutte le cifrature RSA preferite

Include i cifrari nell'ordine seguente:

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

Sì.

Il parametro RSA Preferred di All Ciphers non è rilevante quando CUCM/IMP funge da server. Il CUCM/IMP in quel caso risponde con un tipo di certificato che ha la massima priorità nel messaggio Hello del client?

Sì.

Se questo parametro si riferisce solo a SIP/CTI, esiste un parametro equivalente per le connessioni TLS con interfacce XMPP?

No. Esiste un miglioramento della funzionalità per XMPP, ma non è ancora implementato.