IM and Presence和ECDSA證書問題與解答

目錄

簡介

本文回答有關與Cisco IM and Presence(IM&P)裝置配合使用的橢圓曲線數位簽章演算法(ECDSA)證書的問題。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)
- Cisco IM和狀態(IMP)
- 作業階段啟始通訊協定(SIP)
- 電腦電話整合(CTI)
- Rivest-Shamir-Adleman(RSA)加密
- 橢圓曲線數位簽章演算法(ECDSA)
- 可擴充訊息和狀態通訊協定(XMPP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IM和狀態版11.5.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

IM&P產品團隊關於ECDSA的討論

參照企業引數傳輸層安全性(TLS)密碼，預設選擇為「所有密**碼RSA首選」**。因此，在參考TLS引數密碼時，IM&P工程團隊提出了以下問題。

附註：IM&P工程團隊會回答並驗證所有問題。

此引數是否指示IM&P挑選RSA是否必須在RSA和ECDSA之間進行選擇？

會。此引數僅適用於CUCM SIP/CTI介面。 與ECDSA相比，RSA密碼具有優先權。

Cisco IM and Presence可以在什麼條件下傳送ECDSA（即使已選擇所有密碼RSA Preferred）？

它用於優先使用RSA密碼，但它也具有ECDSA密碼，但當客戶端發起連線時，它會將RSA密碼傳送到ECDSA之上。

如果ECDSA具有更高的優先順序，那麼即使選擇了「所有密碼RSA首選」，是否可以選擇它？

會。只有當CUCM充當客戶端時，此引數才會進入圖片。優先使用順序為客戶端發起連線的順序。如果使用者端使用頂部的ECDSA密碼發起連線，則會使用ECDSA進行連線。如果不是，則賦予RSA優先順序。

可以明顯選擇哪些密碼具有最高優先順序。當第三方客戶端傳送帶有其密碼套件的Hello消息時，Cisco IM and Presence是否從伺服器和客戶端都支援的第三方客戶端TLS密碼對映頁面上的此清單中選擇最強密碼？

會。當伺服器作為使用者端時，會按照前面問題中提到的順序傳送密碼。

是否有任何文檔可以澄清這些事情？

會。在企業引數頁上選擇「**TLS密碼」**連結後，就會出現一個幫助選項，該連結會說明支援的密碼清單。

只有當CUCM/IMP充當客戶端時，所有密碼RSA Preferred引數才重要？

會。

這是否意味著CUCM/IMP（客戶端）同時傳送RSA和ECDSA證書，但RSA證書可以具有最高的優先順序？

會。

在TLS密碼幫助頁面上，它表示此順序中包含密碼。這是否意味著選中此選項時，會按該順序傳送密碼？

所有密碼RSA首選

按以下順序包括密碼：

TLS_ECDHE_RSA with AES256_GCM_SHA384

使用AES256_GCM_SHA384的TLS_ECDHE_ECDSA

TLS_ECDHE_RSA with AES128_GCM_SHA256

使用AES128_GCM_SHA256的TLS_ECDHE_ECDSA

TLS_RSA with AES_128_CBC_SHA1

會。

當CUCM/IMP充當伺服器時，「All Ciphers RSA Preferred」引數並不重要。在這種情況下，CUCM/IMP會使用客戶端Hello消息中優先順序最高的證書型別進行響應？

會。

如果此引數僅引用SIP/CTI，則對於具有XMPP介面的TLS連線，是否存在等效引數？

沒有。XMPP的功能增強，但尚未實施。