IM and Presence和ECDSA证书问题和答案

目录

简介

本文档回答与与思科即时消息和在线状态(IM&P)设备配合使用的椭圆曲线数字签名算法(ECDSA)证书相关的问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器 (CUCM)
- 思科即时消息和在线状态(IMP)
- 会话初始协议 (SIP)
- 计算机电话集成(CTI)
- Rivest-Shamir-Adleman(RSA)加密
- 椭圆曲线数字签名算法(ECDSA)
- 可扩展消息传送和网真协议 (XMPP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科即时消息和在线状态11.5.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

ECDSA的IM&P产品团队讨论

参考企业参数传输层安全(TLS)密码，默认选择为“所有密**码RSA首选”**。因此，在参数TLS密码中，IM&P工程团队提出了以下问题。

> **注意**：所有问题均由IM&P工程团队回答并验证。

如果IM&P必须在RSA和ECDSA之间进行选择，此参数是否会告知IM&P选择RSA?

Yes.此参数仅用于CUCM SIP/CTI接口。 RSA密码优先于ECDSA。

在什么情况下，即使选择了“所有密码RSA首选”，思科即时消息和在线状态也可以发送ECDSA?

它用于提供对RSA密码的优先级，但它也具有ECDSA密码，但当客户端发起连接时，它会在ECDSA上方发送RSA密码。

如果ECDSA具有更高的优先级，是否可以选择它，即使选择了All Ciphers RSA Preferred?

Yes.此参数仅在CUCM充当客户端时才出现在图片中。根据客户端发起连接的顺序指定优先级。 如果客户端启动与顶部ECDSA密码的连接，则使用ECDSA进行连接。否则，RSA优先。

显然，可以选择哪些密码具有最高优先级。当第三方客户端发送Hello消息及其密码套件时，Cisco IM and Presence是否会从此列表中为服务器和客户端都支持的第三方客户端TLS密码映射页面选择最强的密码？

Yes.当服务器充当客户端时，它会按前面问题中提到的顺序发送密码。

是否有任何文档可以阐明这些内容？

Yes.在企业参数页面上选择**TLS密码**链接后，即会出现一个帮助选项，该页面会列出支持的密码。

所有密码RSA首选参数仅在CUCM/IMP充当客户端时才重要？

Yes.

这是否意味着CUCM/IMP（客户端）同时发送RSA和ECDSA证书，但RSA证书可以具有最高优先级？

Yes.

在TLS密码帮助页面上，它表示密码包含在此顺序中。这是否意味着选择此选项时按该顺序发送密码？

所有密码RSA首选

按以下顺序包括密码：

带AES256_GCM_SHA384的TLS_ECDHE_RSA

带AES256_GCM_SHA384的TLS_ECDHE_ECDSA

带AES128_GCM_SHA256的TLS_ECDHE_RSA

带AES128_GCM_SHA256的TLS_ECDHE_ECDSA

带AES_128_CBC_SHA1的TLS_RSA

Yes.

当CUCM/IMP充当服务器时，All Ciphers RSA Preferred参数并不重要。在这种情况下，CUCM/IMP会以在客户端的Hello消息中具有最高优先级的证书类型做出响应？

Yes.

如果此参数仅指SIP/CTI，是否有与XMPP接口的TLS连接的等效参数？

否。XMPP有功能增强功能，但尚未实施。