Crittografa e decrittografa IM&P Conformità Chiave di crittografia

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Premesse](#)

[Crittografia/decrittografia](#)

[Risoluzione dei problemi](#)

[Procedure ottimali per la sicurezza](#)

Introduzione

In questo documento viene descritto come crittografare e decrittografare la chiave di crittografia generata da IM&P per la configurazione con conformità crittografata.

Prerequisiti

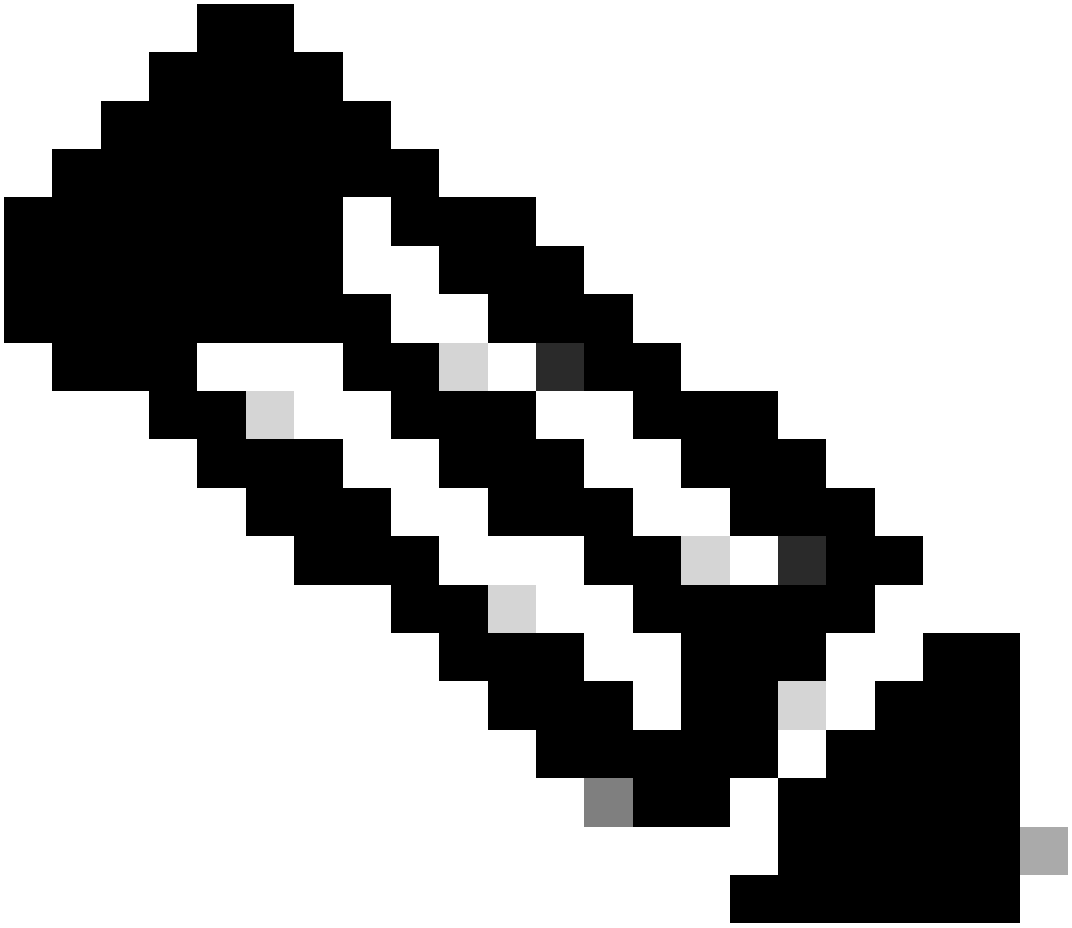
Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione archivio messaggi
- OpenSSL

Componenti usati

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

- MacOS 15.5
- IM and Presence(IM&P) versione 15su2
- OpenSSL 3.3.6



Nota: I comandi mostrati in questo documento possono variare a seconda della versione o della piattaforma OpenSSL in uso. Internet è una buona fonte per trovare coloro che si adattano al vostro ambiente.

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.

Premesse

La funzione di archiviazione dei messaggi fornisce una soluzione di base per la conformità IM. Questa funzionalità consente al sistema di essere conforme alle normative che richiedono la registrazione di tutto il traffico di messaggistica immediata nella società. Molti settori richiedono che i messaggi immediati rispettino le stesse linee guida di conformità alle normative vigenti per tutti gli altri record aziendali. Per garantire la conformità a queste normative, il sistema deve

registrare e archiviare tutti i record aziendali e i record archiviati devono essere recuperabili.

Per una maggiore protezione, è possibile attivare un database crittografato per il programma di archiviazione messaggi. Quando questa opzione è abilitata, il servizio di messaggistica immediata e presenza crittografa i messaggi istantanei prima di archiviarli nel database esterno. Con questa opzione, tutti i dati nel database vengono crittografati e non è possibile leggere i messaggi istantanei archiviati, a meno che non si disponga della chiave di crittografia.

La chiave di crittografia può essere scaricata dal servizio di messaggistica istantanea e presenza e utilizzata in combinazione con qualsiasi strumento utilizzato per visualizzare i dati allo scopo di decrittografare i dati archiviati.

Crittografia/decrittografia

1. Aprire il terminale OpenSSL.
2. Genera chiave privata.

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

3. Estrarre la chiave pubblica dalla chiave privata.

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

4. A questo punto, sono disponibili 2 file private_key.pem e public_key.pem.

- chiave_privata.pem: Consente di decrittografare la chiave crittografata da IM&P.
- chiave_pubblica.pem: Questa è la chiave che si condivide con il server IM&P per consentire loro di crittografare la chiave AES e IV.

Inoltre, il server IM&P aggiunge la codifica Base64 alla chiave di crittografia crittografata.

5. Scaricare la chiave di crittografia dal server IM&P. Fare riferimento alla sezione Download Encryption Key nella guida Instant Messaging Compliance Guide (Guida alla conformità della messaggistica istantanea per i servizi di messaggistica istantanea e presenza).
6. A questo punto sono disponibili 3 file: private_key.pem, public_key.pem e encrypted_key.pem.
7. In questo caso, encrypted_key.pem è codificato in Based64 per una trasmissione sicura.
8. Decodificare la chiave crittografata con codifica Base64.

```
base64 -D -i encrypted_key.pem -o encrypted_key.bin
```

In questo modo viene rimossa la codifica Base64 e viene generato un file da 256 byte che è stato originariamente crittografato con la chiave RSA pubblica.

9. Decrittografare la chiave crittografata con la chiave privata RSA.

```
openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted_key.bin -out decryptedkey.bin
```

In questo modo vengono decrittografate le chiavi AES (K) e IV utilizzate per la crittografia dei messaggi IM&P.

Esempio di file decrittografato:

key = 0ec39f2a22abf63d4452b932f12de

iv = 683 bb3d7e59e82e3fa9f42

10. Decrittografare i messaggi crittografati con AES.

```
openssl enc -aes-256-cbc -d -in encrypted.bin -out decrypted.txt -K <hex_key> -iv <hex_iv>
```

Risoluzione dei problemi

Di seguito è riportato un errore comune durante il tentativo di decrittografare il file crittografato:

```
Public Key operation error 60630000:error:0200006C:rsa routines:rsa_ossl_private_decrypt:data greater t
```

Questo errore si verifica quando si tenta di decrittografare con RSA dati troppo grandi per la dimensione della chiave privata RSA. RSA può decrittografare dati solo fino alla dimensione del modulo. Nel nostro caso, una chiave RSA a 2048 bit può decrittografare solo 256 byte.

Se si controlla il file di chiave crittografata generato da IM&P, sono necessari 344 byte. È possibile decrittografare solo 256 byte con la nostra chiave privata.

```
-rw-rw-rw-@ 1 testuser staff 344 Jun 5 13:10 encrypted_key.pem
```

Come accennato in precedenza in questo documento, la chiave crittografata è codificata in Base64 per una trasmissione sicura, che aggiunge byte alle dimensioni del file.

Una volta rimossa la codifica Base64, si dispone di un file da 256 byte, facilmente decrittografabile con la nostra chiave privata.

```
-rw-r--r-- 1 testuser staff 256 Jun 12 09:16 encrypted_key.bin
```

Procedure ottimali per la sicurezza

- Archiviare la chiave privata (private_key.pem) in modo sicuro.
- Non condividere la chiave privata con altri utenti né caricarla in sistemi non attendibili.
- Pulisci i file temporanei come decryptedkey.bin dopo la decrittografia.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).