

排除PQC PPK手動金鑰十六進位制格式解析器拒絕故障

目錄

問題

當在Cisco IOS XE上使用十六進位制格式的PQC (量子後加密) 和手動PPK (量子後預共用金鑰) 配置[IPsec](#) (IP安全) 時，裝置可以拒絕十六進位制格式的PPK，但有以下任一錯誤：

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5
```

```
% Invalid input detected at '^' marker.
```

```
Device(config-ikev2-keyring-peer)#
```

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c88
```

```
% Invalid hex key.All characters in hex string must be ASCII.
```

```
Device(config-ikev2-keyring-peer)#
```

環境

- 執行Cisco IOS XE軟體的Cisco路由器
- IPsec使用量子後密碼實現和手動PPK金鑰

解析

路由器使用PPK手動金鑰配置的十六進位制字串驗證解碼的位元組值。已解碼的值必須滿足以下兩個要求：

- 十六進位制編碼的PPK必須表示有效的ASCII字串。由於每個ASCII字元使用8位進行編碼，並且每個十六進位制字元代表4位資訊，因此輸入十六進位制字串必須包含偶數字元。例如，十六進位制字串3a4b5是無效的輸入，因為它有一個奇數(5)的十六進位制字元。
- 僅當解碼的位元組保留在標準ASCII位元組範圍(0x00-0x7F)內時，解析器才接受十六進位制值。有問題的金鑰3a4b5c88被拒絕，因為：

```
0x3a = 58 (ascii ":") valid
0x4b = 75 (ascii "K") valid
0x5c = 92 (ascii "\") valid
0x88 = 136 invalid - outside of standard ASCII range
```

要解決此錯誤，請使用十六進位制值，其中每個位元組都保留在標準ASCII範圍(0x00-0x7F)內，例如：

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c88
% Invalid hex key.All characters in hex string must be ASCII.
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c78
Device(config-ikev2-keyring-peer)#
```

原因

十六進位制格式的PPK鍵輸入無效，因為它超出了標準[ASCII字元](#)範圍(0x00-0x7F)。

相關內容

- [使用後量子預共用金鑰配置量子安全加密](#)
- '思科錯誤ID [CSCwn32983](#)' (使用思科內部錯誤來更清楚顯示分析器錯誤)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。