

PQC PPKの手動キーの16進数形式パーサー拒否のトラブルシューティング

内容

お問い合わせ内容

Cisco IOS XEで、PQC(Post-Quantum Cryptography)および手動PPK(Post-Quantum Pre-shared Keys)を16進形式で使用して[IPsec](#)(IP Security)を設定する場合、デバイスは次のエラーのいずれかで16進形式のPPKを拒否できます。

```
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

- Cisco IOS XEソフトウェアを実行するシスコルータ
- 手動PPKキーによるPost-Quantum Cryptography(PQC)実装を使用したIPSec

解決策

ルータは、PPKの手動キー設定について、デコードされたバイト値を16進数文字列で検証します

。デコードされた値は、次の2つの要件を満たしている必要があります。

- 16進数にエンコードされたPPKは、有効なASCII文字列を表す必要があります。各ASCII文字は8ビットを使用してエンコードされ、16進文字は4ビットの情報を表すので、入力16進文字列は偶数の文字で構成される必要があります。たとえば、16進数文字列3a4b5は、16進数の奇数(5)であるため、無効な入力です。
- デコードされたバイトが標準のASCIIバイト範囲(0x00-0x7F)内に残っている場合にのみ、パーサーは16進値を受け取ります。問題のあるキー3a4b5c88は次の理由で拒否されました。

```
0x3a = 58 (ascii ":") valid
0x4b = 75 (ascii "K") valid
0x5C = 92 (ascii "\") valid
0x88 = 136 invalid - outside of standard ASCII range
```

このエラーを解決するには、各バイトが標準ASCII範囲(0x00-0x7F)内に収まる16進数値を使用します。次に例を示します。

```
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

16進数形式の無効なPPKキー入力です。[標準のASCII文字範囲\(0x00-0x7F\)](#)外です。

関連コンテンツ

- [Postquantum事前共有キーを使用したQuantum-Safe暗号化の設定](#)
- 『Cisco Bug ID [CSCwn32983](#)』（パーサーエラーをより明確にするためのシスコ内部のバグ）
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。