

Risoluzione dei problemi relativi al rifiuto del parser per il formato esadecimale della chiave PPK di PQC manuale

Sommario

Problema

Quando si [configura IPsec](#) (IP Security) su Cisco IOS XE con PQC (Post-Quantum Cryptography) e PPK manuale (Post-Quantum Pre-shared Keys) in formato esadecimale, il dispositivo può rifiutare il formato esadecimale PPK con uno dei seguenti errori:

```
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)#
```

Ambiente

- Router Cisco con software Cisco IOS XE
- IPsec con implementazione della crittografia post-quantistica con chiavi PPK manuali

Risoluzione

Il router convalida i valori byte decodificati con stringhe esadecimali per la configurazione della chiave manuale PPK. Il valore decodificato deve soddisfare i seguenti due requisiti:

- Il PPK con codifica esadecimale deve rappresentare una stringa ASCII valida. Poiché ogni carattere ASCII è codificato utilizzando 8 bit e ogni carattere esadecimale rappresenta 4 bit di informazioni, la stringa esadecimale di input deve essere costituita da un numero pari di caratteri. Ad esempio, la stringa esadecimale 3a4b5 non è un input valido perché contiene un numero dispari (5) di caratteri esadecimali.
- Il parser accetta valori esadecimali solo se i byte decodificati rimangono entro l'intervallo di byte ASCII standard (0x00-0x7F). La chiave con problemi 3a4b5c88 è stata rifiutata perché:

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

Per risolvere questo errore, utilizzare valori esadecimali in cui ogni byte rimane all'interno dell'intervallo ASCII standard (0x00-0x7F), ad esempio:

```
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)#
```

Causa

Input del tasto PPK non valido in formato esadecimale perché non rientra nell'intervallo di [caratteri ASCII standard](#) (0x00-0x7F).

Contenuto correlato

- [Configurazione della crittografia Quantum-Safe con chiavi già condivise Postquantum](#)
- 'ID bug Cisco [CSCwn32983](#)' (bug interno Cisco per rendere più chiaro l'errore del parser)

- [Supporto tecnico Cisco e download](#)

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).