

PQC PPK 수동 키 16진수 형식 파서 거부 문제 해결

목차

문제

Cisco IOS XE에서 PQC(Post-Quantum Cryptography) 및 수동 PPK(Post-Quantum Pre-shared Keys)를 사용하여 16진수 형식으로 IPsec(IP Security)을 [구성할](#) 때 디바이스는 다음 오류 중 하나로 16진수 형식 PPK를 거부할 수 있습니다.

```
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)#
```

환경

- Cisco IOS XE 소프트웨어를 실행하는 Cisco 라우터
- 수동 PPK 키와 함께 포스트 양자 암호화 구현을 사용하는 IPsec

해결

라우터는 PPK 수동 키 컨피그레이션에 대해 16진수 문자열로 디코딩된 바이트 값을 검증합니다.

디코딩된 값은 다음 두 요구 사항을 충족해야 합니다.

- 16진수로 인코딩된 PPK는 유효한 ASCII 문자열을 나타내야 합니다. 각 ASCII 문자는 8비트를 사용하여 인코딩되고 각 16진수 문자는 4비트의 정보를 나타내므로, 입력 16진수 문자열은 짝수의 문자로 구성되어야 합니다. 예를 들어 16진수 문자열 3a4b5는 16진수 문자의 홀수(5)를 포함하므로 잘못된 입력입니다.
- 파서는 디코딩된 바이트가 표준 ASCII 바이트 범위(0x00-0x7F) 내에 있는 경우에만 16진수 값을 받습니다. 문제가 되는 키 3a4b5c88이 다음과 같은 이유로 거부되었습니다.

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

이 오류를 해결하려면 각 바이트가 표준 ASCII 범위(0x00-0x7F) 내에 있는 16진수 값을 사용합니다. 예를 들면 다음과 같습니다.

```
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)#
```

원인

[표준 ASCII 문자](#) 범위(0x00-0x7F)를 벗어났기 때문에 16진수 형식의 잘못된 PPK 키 입력입니다.

관련 콘텐츠

- [Postquantum 사전 공유 키를 사용하여 Quantum Safe 암호화 구성](#)
- 'Cisco 버그 ID [CSCwn32983](#)'(파서 오류를 보다 명확하게 하는 Cisco 내부 버그)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.