

排除PQC PPK手动密钥十六进制格式解析器拒绝故障

目录

问题

在Cisco IOS XE上配置[IPsec](#) (IP安全) 时，如果采用十六进制格式的PQC (量子后加密) 和手动PPK (量子后预共享密钥)，设备可能会拒绝十六进制格式的PPK，但会出现以下错误之一：

```
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)#
```

环境

- 运行Cisco IOS XE软件的Cisco路由器
- IPsec，使用量子后加密技术实施手动PPK密钥

分辨率

路由器使用PPK手动密钥配置的十六进制字符串验证解码的字节值。解码的值必须满足以下两个要求：

- 十六进制编码的PPK必须代表有效的ASCII字符串。由于每个ASCII字符使用8位进行编码，并且每个十六进制字符代表4位信息，因此输入的十六进制字符串必须包含偶数个字符。例如，十六进制字符串3a4b5是无效输入，因为它有一个奇数(5)的十六进制字符。
- 仅当解码的字节保持在标准ASCII字节范围(0x00-0x7F)内时，解析器才接受十六进制值。有问题的密钥3a4b5c88被拒绝，因为：

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

要解决此错误，请使用十六进制值，其中每个字节都保留在标准ASCII范围(0x00-0x7F)内，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

十六进制格式的PPK密钥输入无效，因为它不在标准ASCII字符范围(0x00-0x7F)之外。

相关内容

- [使用Postquantum预共享密钥配置量子安全加密](#)
- 'Cisco Bug ID [CSCwn32983](#)' (Cisco内部Bug可使解析器错误更加清晰)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。