

### 组网及说明

无

### 问题描述

SSH无法登录

### 过程分析

debug ssh server看

```
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Peer proposal kex:
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(0): diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(1): ssh-dss,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,x509v3-sign-rsa,x509v3-sign-dss
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(2): aes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc,twofish-cbc,blowfish-cbc,3des-cbc,arcfour
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(3): aes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc,twofish-cbc,blowfish-cbc,3des-cbc,arcfour
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(4): hmac-sha2-512,hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,umac-64@openssh.com
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(5): hmac-sha2-512,hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,umac-64@openssh.com
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(6): none
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(7): none
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(8):
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex strings(9):
*May 14 19:34:02:715 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex: client->server, Encrypt: aes256-ctr, HMAC: hmac-sha2-512, Compress: none
*May 14 19:34:02:716 2020 CS-FR-SL-R2 SSSH/7/EVENT: Kex: server->client, Encrypt: aes256-ctr, HMAC: hmac-sha2-512, Compress: none
*May 14 19:34:02:781 2020 CS-FR-SL-R2 SSSH/7/EVENT: Expecting packet type 30.
*May 14 19:34:02:781 2020 CS-FR-SL-R2 SSSH/7/MESSAGE: Received packet type 30.
*May 14 19:34:02:853 2020 CS-FR-SL-R2 SSSH/7/ERROR: Fatal error occurs: unexpected internal error.
%May 14 19:34:02:853 2020 CS-FR-SL-R2 SSSH/6/SSHS_DISCONNECT: SSH user (null) (IP: 22.89.5.155) disconnected from the server.
到交互算法之后报错，遇到了未知的内部错误
```

### 解决方法

经确认现场是通过CRT登录  
设备这边dsa如果配置成为2048位，使用CRT通过SSH登录就会失败。  
DSA改为默认配置后正常登录