**Disable CBC mode cipher encryption**

**And**

**Enable CTR or GCM cipher mode encryption.**

**Remove to disable the below listedalgorithms if available in the following 2 files**

**/etc/ssh/sshd\_config**

**/etc/ssh/ssh\_config**

The following client-to-server Cipher Block Chaining (CBC) algorithms  
are supported :  
  
3des-cbc   
aes128-cbc  
aes192-cbc  
aes256-cbc  
blowfish-cbc  
cast128-cbc  
  
The following server-to-client Cipher Block Chaining (CBC) algorithms  
are supported :  
  
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
blowfish-cbc  
cast128-cbc

**Enable CTR or GCM cipher mode encryption**

Added the this line to /etc/ssh/sshd\_config and /etc/ssh/ssh\_config then restarted sshd, systemctl restart sshd  
  
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,[aes128-gcm@openssh.com](mailto:aes128-gcm@openssh.com),[aes256-gcm@openssh.com](mailto:aes256-gcm@openssh.com)

Restart the sshd services

For RHEL : systemctl restart sshd