Case 03774749

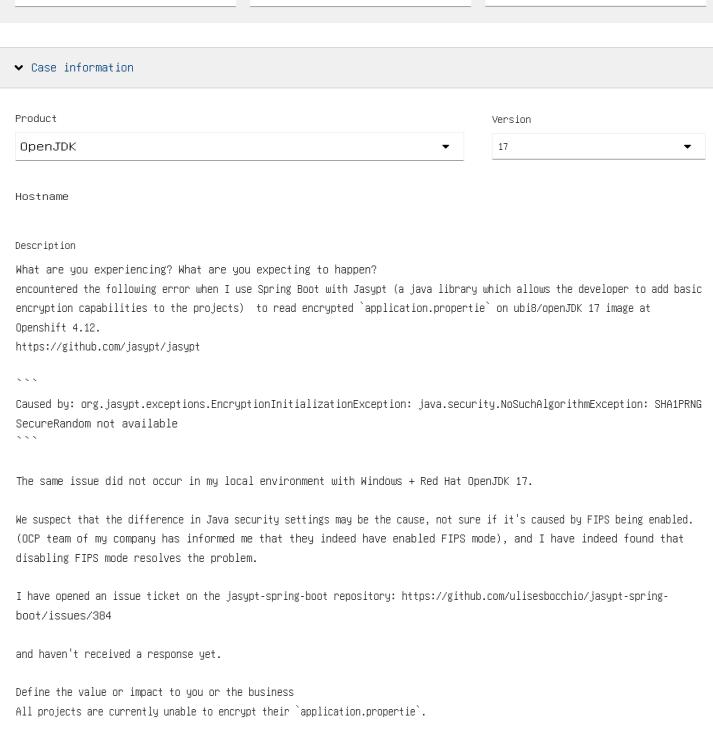
SHA1PRNG SecureRandom not available on RHEL ubi8 image

Product Account Created by

OpenJDK 6399269 TSUNG JUI WU

17 Dynasafe Technologies, Inc. Mar 26, 2024, 07:34:09 AM





I would like to inquire with Red Hat. If it is confirmed that FIPS mode is causing the issue, what would you recommend us to do?

Show more

Discussion

Singh, Rishabh

Tue, Mar 26, 2024, 01:02:09 PM GMT+8

Hi Team,

Thank you.

Thank you for contacting Red Hat Technical Support. My name is Rishabh and I will be supporting on this case.

From case description I understand that you are using Jasypt library to allow encryption capabilities in your application. The application is using ubi8/OpenJDK17 and is deployed on Openshift 4.12.

The application is deployed on FIPS enabled OCP cluster where following error is observed:

Caused by: org.jasypt.exceptions.EncryptionInitializationException: java.security.NoSuchAlgorithmException: SHA1PRNG SecureRandom not available

The issue is resolved when disabling FIPS for the application.

< I would like to inquire with Red Hat. If it is confirmed that FIPS mode is causing the issue, what would you recommend us to do?</p>

> The error suggests SHA1PRNG algorithm is unavailable in available list of algorithm within your application environment. As you have mentioned the issue happens only when FIPS mode is enabled - it suggests that the algorithm might not be available in FIPS mode. The list of available algorithm can be checked by using following code[1] in your application environment: https://access.redhat.com/solutions/7049130

The issue should be resolved by using one of the available Random generator algorithm. The issue is specific to the Jasypt library (external to Red Hat) - the library has to be updated to consider this FIPS use case - where SHA1PRNG random generator algorithm is disabled in FIPS environment.

```
Rishabh
[1]
import java.security.Security;
import java.security.Provider;
public class ShowSecurityAlgorithms {
 public static void main(String[] args){
    for (Provider provider : Security.getProviders()) {
      for (Provider.Service service : provider.getServices()) {
         String algorithm = service.getAlgorithm();
          System.out.println(algorithm);
```



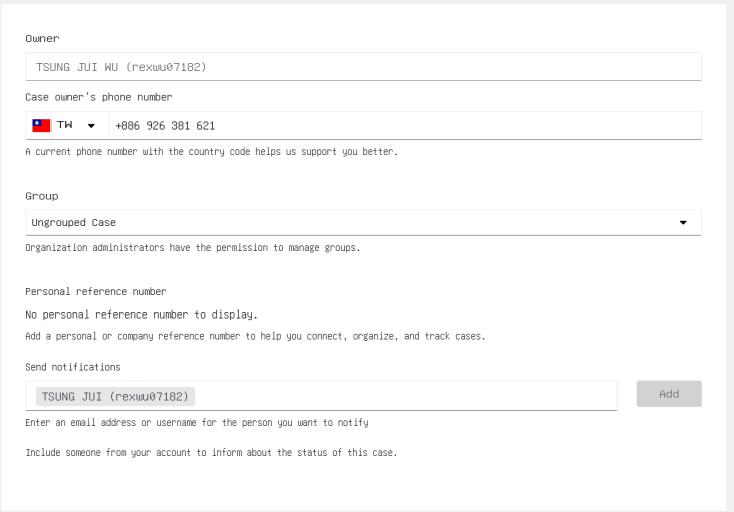








Management



Action plan

No action plan to display.

Private Notes
Please note, contents of this field are not visible to Red Hat Support professionals.