

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

Status

Waiting on Customer

Support type

Configuration

Severity

2 (High) - Production has been seve

▼ Case information

Product

OpenJDK

Version

17

Hostname

Description

What are you experiencing? What are you expecting to happen?

encountered the following error when I use Spring Boot with Jasypt (a java library which allows the developer to add basic encryption capabilities to the projects) to read encrypted `application.propertie` on ubi8/openJDK 17 image at Openshift 4.12.

<https://github.com/jasypt/jasypt>

```

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

```

The same issue did not occur in my local environment with Windows + Red Hat OpenJDK 17.

We suspect that the difference in Java security settings may be the cause, not sure if it's caused by FIPS being enabled. (DCP team of my company has informed me that they indeed have enabled FIPS mode), and I have indeed found that disabling FIPS mode resolves the problem.

I have opened an issue ticket on the jasypt-spring-boot repository: <https://github.com/ulisesbocchio/jasypt-spring-boot/issues/384>

and haven't received a response yet.

Define the value or impact to you or the business

All projects are currently unable to encrypt their `application.propertie`.

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 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?

> 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.

Thank you,
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);
            }
        }
    }
}
```

~~~~



 WU, TSUNG JUI

Tue, Mar 26, 2024, 07:34:24 AM GMT+8

Attached file  [wise2-customer-service-v1-6758958fdf-2qhx1-wise2-customer-service.log \(213.6 KB\)](#) this case.

SHA-256

ac44b9cfc605393efdc241c2239db4161d269a8762e3a2be06b14be5dbb970ee

Description



Management

Owner

TSUNG JUI WU (rexwu07182)

Case owner's phone number

 TW ▼

+886 926 381 621

A current phone number with the country code helps us support you better.

Group

Ungrouped Case ▼

Organization administrators have the permission to manage groups.

Personal reference number

No personal reference number to display.

Add a personal or company reference number to help you connect, organize, and track cases.

Send notifications

TSUNG JUI (rexwu07182)

Add

Enter an email address or username for the person you want to notify

Include someone from your account to inform about the status of this case.

Action plan

No action plan to display.

Private Notes

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