CVE 2022 45146

Jump to bottom

David Hook edited this page 12 days ago · 7 revisions

Issue affecting: BC-FJA 1.0.2.3 and earlier.

Fixed versions: BC-FJA 1.0.2.4, BC-FJA 2.0.0

Platform affected: Java 13 and later.

As of Java 13 a change in the garbage collector has meant that the garbage collector will call finalize() and sometimes partially or totally zero out internal keys in the FIPS module while methods on the keys are still in use but the objects themselves are not reachable. This behavior is within the bounds of the language specification. For the curious there is long discussion on this very topic as well as how to prevent it in the JavaDoc discussion in Reference.reachabilityFence().

As the problem is internal, the behavior can result in encryption, decryption, and authentication failures, for example an exchanged key will have the value expected, but its internal representation on either end may be corrupted as it is passed around inside the module. There is also a risk of information disclosure prior to the failure making itself visible as the key may end up being all zeroes. The interaction is not observed prior to Java 13. Testing has shown the issue is most evident when the JVM is stressed for memory but as there is a chance of it happening even during normal usage the BC FIPS modules should not be used on Java 13 or later. As the module has not been certified for use with these JVMs a non-certified release candidate has been made available on the latest releases page for those wishing to make use of the jar on later JVMs such as Java 17.

BC-FJA 1.0.2.3 and earlier are certified for use with Java 7, Java 8, and in the case of the 1.0.2 series Java 11. This issue **does not** apply where the modules are used on the JVMs that they were tested and certified on.

There is a demo program showing the problem in the file gctest.zip. To run the demo unzip the demo file in the current directory and get a copy of bc-fips-1.0.2.3.jar, then with Java 17 execute the following:

```
javac -d classes -cp bc-fips-1.0.2.3.jar gctest/*.java
java -Xmx200M -cp bc-fips-1.0.2.3.jar:classes gctest.Main 15 1000
```

It usually fails within 100 tests.

We wish to gratefully acknowledge the work of Jakub Trávník from Broadcom in identifying and reporting this problem and providing the sample program.