**Problem**

CVE-2016-1000352: In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.

CVE-2016-1000344: In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.

[https://github.com/bcgit/bc-java/blob/master/core/src/main/java/org/bouncycastle/crypto/engines/**AESEngine.java**](https://github.com/bcgit/bc-java/blob/master/core/src/main/java/org/bouncycastle/crypto/engines/AESEngine.java)

‘Graphical user interface, text, application

Description automatically generated

**dh\_IESCipher.java && ec\_IESCipher.java**

import org.bouncycastle.crypto.engines.**AESEngine**;

**AESEngine.java**

public class AESEngine

**extends DefaultMultiBlockCipher**

/\*\* Return an AESEngine.

\* @**return an AES ECB mode cipher**.

\*/

public static MultiBlockCipher newInstance()

{

return new AESEngine();

}

/\*\*

**Fix**

[https://github.com/bcgit/bc-java/blob/master/core/src/main/java/org/bouncycastle/crypto/engines/**AESFastEngine.java**](https://github.com/bcgit/bc-java/blob/master/core/src/main/java/org/bouncycastle/crypto/engines/AESFastEngine.java)

**dh\_IESCipher.java && ec\_IESCipher.java**

import org.bouncycastle.crypto.engines.**AESFastEngine**;

**AESFastEngine.java**

public class AESFastEngine

**implements BlockCipher**