hycxss

654 0

分享时间: 2021.04.15

There is a deserialization vulnerability in jfinal using redis

Github：https://github.com/jfinal/jfinal

Jfinal is a popular java web development framework with 3000 stars

https://github.com/jfinal/jfinal/blob/master/src/main/java/com/jfinal/plugin/redis/serializer/JdkSerializer.java

Line 67

```
public Object valueFromBytes(byte[] bytes
    if(bytes == null || bytes.length == 0)
        return null;

    ObjectInputStream objectInput = null;
    try {
        ByteArrayInputStream bytesInput = r
        objectInput = new ObjectInputStream
        return objectInput.readObject();
    }
    catch (Exception e) {
        throw new RuntimeException(e);
    }
    finally {
        if (objectInput != null)
            try {objectInput.close();} catch
    }
}
```

If the bytecode is maliciously generated by ysoserial, it will cause the vulnerability of remote code execution

https://github.com/jfinal/jfinal/blob/master/src/main/java/c