@CallerSensitive一些理解

王侦 关注

0.596 2019.06.21 20:22:14 字数 215 阅读 1,010

```
@CallerSensitive
public static Lookup lookup() {
    return new Lookup(Reflection.getCallerClass());
}

@CallerSensitive
public static native Class<?> getCallerClass();
```

JEP 176: Mechanical Checking of Caller-Sensitive Methods中的说明：

```
Improve the security of the JDK's method-handle implementation by replacing
the existing hand-maintained list of caller-sensitive methods with a mechanism
that accurately identifies such methods and allows their callers to be discovered reliably.
```

使用能够精确识别caller-sensitive方法并且保证这些方法的调用者可靠地被发现的一种机制 代替现存的手动维护的caller-sensitive方法表，提高JDK method-handler实现的安全性。

```
A caller-sensitive method varies its behavior according to the class of its immediate caller.
It discovers its caller's class by invoking the sun.reflect.Reflection.getCallerClass method.
```

caller-sensitive方法会根据其直接调用者的类型改变其行为。通过调用sun.reflect.Reflection.getCallerClass方法可以获得调用者class类型。

```
Most caller-sensitive methods act in some way as an agent for the caller.
When invoked via reflection, these methods must be handled specially in order to
ensure that the class of the actual caller, rather than some class of the reflection mechanism i
is returned by the getCallerClass method.
```

大多数caller-sensitive方法某种程度上是作为调用者的代理。当通过反射调用时，这些方法必须经过特殊处理以确保getCallerClass返回的是实际调用者的class类型，而不是反射机制本身的某些类。

另外，据JVM注解@CallSensitive文章，有一个类似的解释：

```
这个注解是为了堵住漏洞用的。曾经有黑客通过构造双重反射来提升权限，
原理是当时反射只检查固定深度的调用者的类，看它有没有特权，
例如固定看两层的调用者（getCallerClass(2)）。如果我的类本来没足够
权限群访问某些信息，那我就可以通过双重反射去达到目的：反射相关
的类是有很高权限的，而在 我->反射1->反射2 这样的调用链上，反射2
检查权限时看到的是反射1的类，这就被欺骗了，导致安全漏洞。
使用CallerSensitive后，getCallerClass不再用固定深度去寻找
actual caller（“我”），而是把所有跟反射相关的接口方法都标注上
CallerSensitive，搜索时凡看到该注解都直接跳过，这样就有效解决了
前面举例的问题

```

官方文档 https://docs.oracle.com/javase/9/whatsnew/toc.htm#JS...

互联网编程 阅读 172 评论 0 赞 1

Effective Java一书笔记

对象的创建与销毁 Item 1: 使用static工厂方法，而不是构造函数创建对象：仅仅是创建对象的方法，并非Fa...

孙小磊 阅读 419 评论 0 赞 1

[1/2]Clojure入门教程: Clojure – Functional Program...

//Clojure入门教程: Clojure – Functional Programming for the J...

葡萄喃喃呓语 阅读 1,051 评论 0 赞 2

java编程学习之反射技术及其应用

Java是一种可以撰写跨平台应用软件的面向对象的程序设计语言。Java 技术具有卓越的通用性、高效性、平台移植性和...

Java小辰 阅读 258 评论 1 赞 2

Java基础知识整理

整理来自互联网 1，JDK：Java Development Kit，java的开发和运行环境，java的开发工具...

Ncompass 阅读 692 评论 0 赞 6