Software Vulnerabilities: Exploitation and Mitigation

—

Lab 8

Alexandre Bartel

The report for the lab should consist of a single pdf file. Please use the following filename:

`lab8_FIRSTNAME_LASTNAME.pdf`

Send the report to alexandre.bartel@uni.lu with the following subject:

`MICS2019SVEM Lab8 FIRSTNAME_LASTNAME`

The deadline is the 12^{th} of May 2019 at 23:59.

1 Lab 8 (23 P.)

In this lab you will exploit a type confusion in the Java virtual machine to bypass the Java sandbox and execute arbitrary code.

1.1 Vulnerable VM

Read the article Sandbox Escape by Type Confusion by Vincent Lee.

Question 1.1 What version(s) of Oracle's Java Virtual Machine is/are vulnerable to CVE-2018-2826? Explain how you did find the answer. 2 P.

1.2 Running the Exploit

Within the VM of Lab 1, download the Java JDK 10 from Oracle's website. The filename is `jdk-10_linux-x64_bin.tar.gz`. Once downloaded, extract the content of the archive:

```
$ tar xzvf jdk-10_linux-x64_bin.tar.gz
```

You can now run the Java 10 virtual machine and the Java 10 compiler using the following commands:

```
$ ./jdk-10/bin/java
$ ./jdk-10/bin/javac
```

You can run the JVM with the security manager turned on and no permissions given to the code with the following command:

```
$ java -Djava.security.manager
```

Question 1.2 Write a java program which creates a new file on the disk. Launch it with the security manager turned on and give no permission to the code. What is the behavior of the VM when the program is run? 2 P.

Question 1.3 Using the code snippets of the article, reconstruct your own class to exploit the vulnerability of CVE-2018-2826. Run the JVM with a security manager and no permission, and show that you can disable the security manager to execute arbitrary code without the required permissions (e.g., try to create a file). 5 P.

1.3 Type Confusion

In the article, there is a type confusion between type `Lookup` and type `LookupMirror`.

Question 1.4 Class `Lookup` is a class of the Java Class Library (JCL). Class `LookupMirror` is a class created by the attacker. The two first fields `lookupClass` and `allowedModes` of each classes are almost the same. Explain the difference. 3 P.

Question 1.5 During the type confusion attack, the attacker writes information to an instance of type A through an instance of type B. In the case of the code from the article, what is type A? What is type B? What is the information written to A? 3 P.

Question 1.6 What is one of the major Java – or more generally speaking object-oriented – concept which the vulnerability breaks (Object, Class, Inheritance, Polymorphism, Abstraction or Encapsulation)? Explain. 3 P.

1.3.1 Patching in a Hurry

Suppose you work for a company which relies on the JVM version 10 to execute jobs (Java programs) from your clients. You know about CVE-2018-2826, but Oracle has not yet deployed a fixed version. As this is critical for the stability and security of your infrastructure, you decide to fix the JVM yourself using the information from the article.

Question 1.7 Explain the patch of class `java/lang/invoke/MethodHandles`. 3 P.

Question 1.8 Briefly explain how you would do to fix the JVM yourself with the patch 2 P.

Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always properly cite your sources.