Software Vulnerabilities: Exploitation and Mitigation

—

Lab 7

Prof. Jacques Klein & Pedro Jesús Ruiz Jiménez
(inspired from Prof. Alexandre Bartel's course)

7 Type Confusion (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.

7.1 Setup Labs Environment

7.1.1 Update resources

From our *Git* directory (`SVEM`), use this command to update the lab resources:

```
$ git pull
```

7.2 Launch Emulated Environment

On your host machine, go to the `Lab07` directory found inside the cloned repository. Then, create the virtual machine (vm) and connect to it by using the following commands:

```
$ vagrant up
$ vagrant ssh
```

Other important vagrant commands that you might need are:

```
$ vagrant halt  # Stops vm
$ vagrant reload  # Resets vm
$ vagrant destroy  # Destroys vm
$ vagrant provision  # Rerun provision
$ vagrant global-status  # Status about vms
```

Finally, once you are connected to the vm, you'll need to move to the work directory: `lab`

7.3 Vulnerable VM

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

Question 7.1 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.

7.4 Running the Exploit

In the host machine, download "Java JDK 10" from Oracle's website inside the `Lab06/lab` directory. Then, in the vm extract its content using the following command:

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

You can now run the Java 10 vm (JVM) and the Java 10 compiler using the following commands:

```
$ jdk-10.0.2/bin/java
$ jdk-10.0.2/bin/javac
```

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

```
$ jdk-10.0.2/bin/java -Djava.security.manager
```

Question 7.2 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 7.3 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.

7.5 Type Confusion

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

Question 7.4 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 7.5 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 7.6 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.

7.5.1 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 7.7 Explain the patch of class `java/lang/invoke/MethodHandles`. 3 P.

Question 7.8 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 cite the source from which you obtained the text.