Apache Tomcat RCE by deserialization

CVE-2020-9484

Yadhu Krishna M
2nd year, CSE

Prerequisites

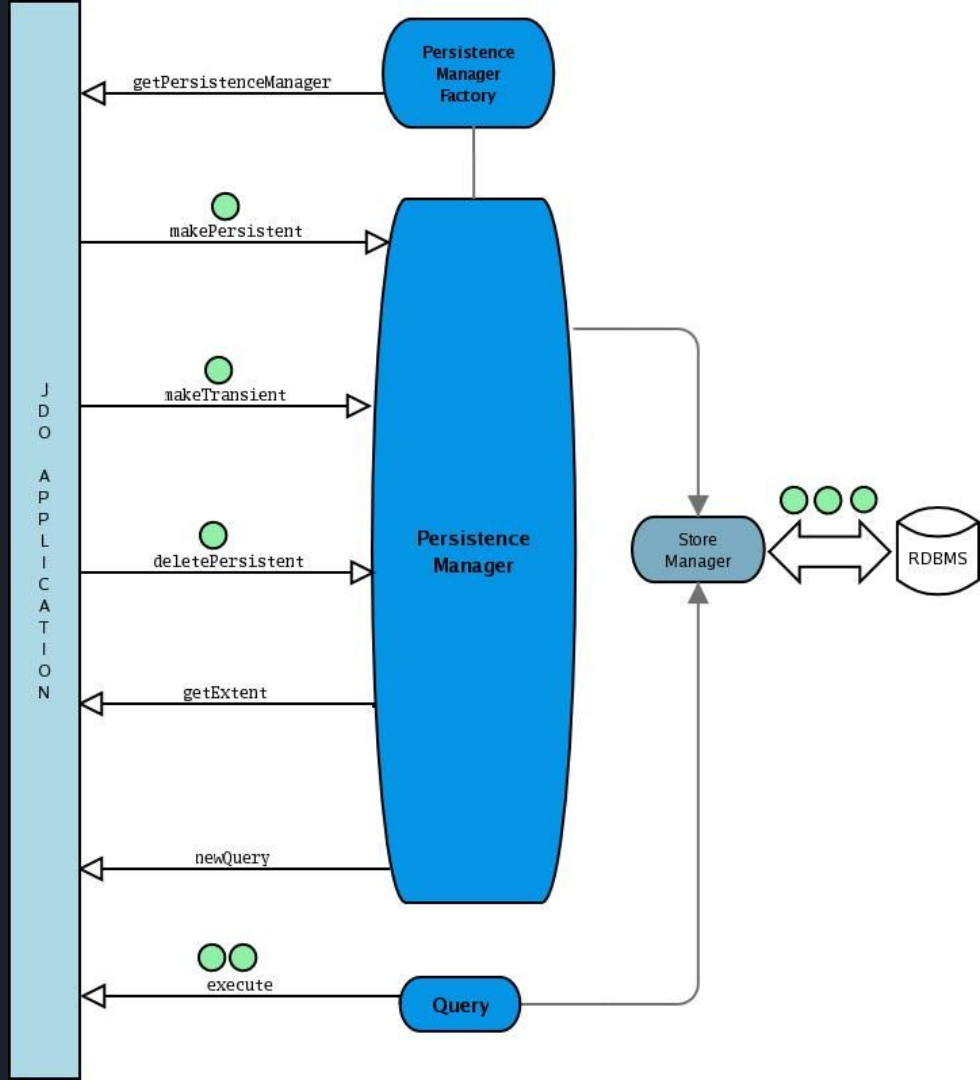
01 The PersistentManager is enabled and should be using a FileStore.

02 Attacker should be able to upload arbitrary files and should know file name and location.

03 There are gadgets in the classpath that can be used for a Java deserialization attack.

The Persistent Manager

1. Key interface for JDO-aware application components.
2. Manages sessions.
3. Sessions used to preserve state between client requests

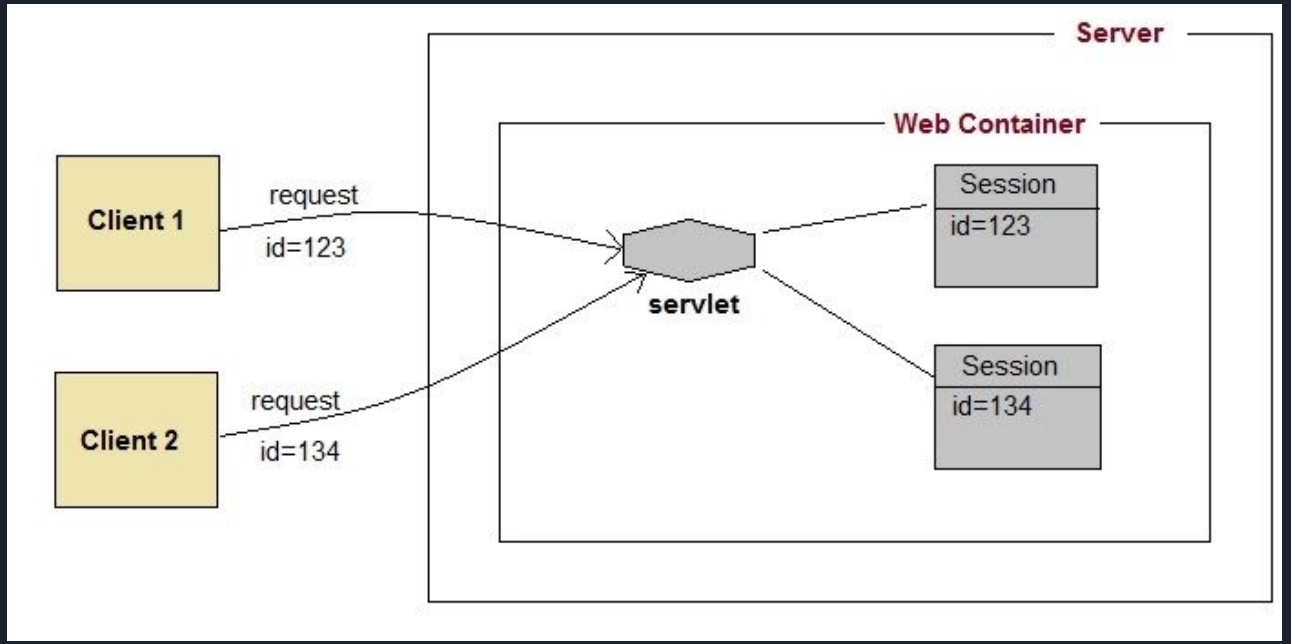


What does a Session Manager do?

1. Storage location
2. Storage format
3. Generation of Session IDs
4. Session Attributes

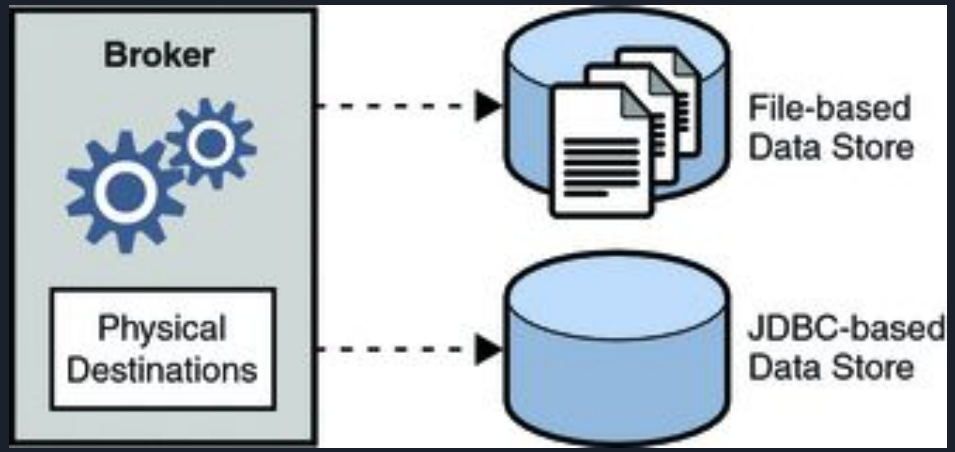
Tomcat provides two implementations:

1. org.apache.catalina.session.**StandardManager** (Default)
2. org.apache.catalina.session.**PersistentManager** (Target)



Storing sessions using PersistentManager

1. **FileStore:** Swapped sessions stored as file with the name based on the session ID
2. **JDBCStore:** Stores in the database. Each swapped session will be stored as individual row.



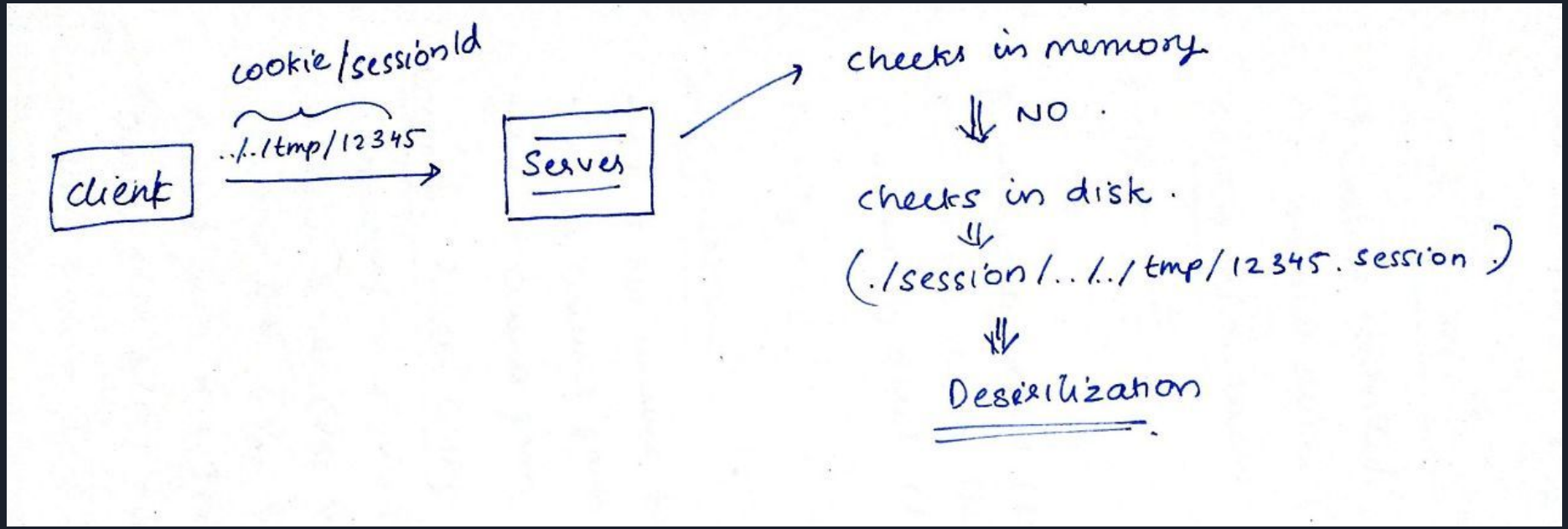
How to enable PersistentManager?

conf/context.xml

```
<Manager className="org.apache.catalina.session.PersistentManager"
         maxIdleSwap="15">
  <Store className="org.apache.catalina.session.FileStore"
         directory="./session/" />
</Manager>
```

The Exploit !

PersistentManager



```
java.io.ObjectInputStream.readSerialData(ObjectInputStream.java:2235)
java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:2126)
java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1625)
java.io.ObjectInputStream.readObject(ObjectInputStream.java:465)
java.io.ObjectInputStream.readObject(ObjectInputStream.java:423)
org.apache.catalina.session.StandardSession.doReadObject(StandardSession.java:1545)
org.apache.catalina.session.StandardSession.readObjectData(StandardSession.java:1040)
org.apache.catalina.session.FileStore.load(FileStore.java:229)
org.apache.catalina.session.PersistentManagerBase.loadSessionFromStore(PersistentManagerBase.java:764)
org.apache.catalina.session.PersistentManagerBase.swapIn(PersistentManagerBase.java:714)
org.apache.catalina.session.PersistentManagerBase.findSession(PersistentManagerBase.java:493)
```

- Tries to read data.
- Tries to unserialize it.
- Loads session from file

References

1. https://books.google.co.in/books?id=ooInCgAAQBAJ&pg=PA124&lpg=PA124&dq=persistencemanager+filestore&source=bl&ots=QKfVSeLXXn&sig=ACfU3U2C0Wdz76lvLts5Qvq9GmtbKZncAA&hl=en&sa=X&ved=2ahUKEwiiwdLS4PfpAhXISH0KHVdKAQQQ6AEwB3oECAkQAQ#v=onepage&q=persistencemanager%20filestore&f=false
2. https://www.service-architecture.com/articles/database/jdo_persistence_manager.html
3. https://docs.oracle.com/cd/E19651-01/817-2149-10/dwsessn.html
4. https://www.redtimmy.com/java-hacking/apache-tomcat-rce-by-deserialization-cve-2020-9484-write-up-and-exploit/