CVE漏洞扫描插件

一、原理说明

有一帮用爱发电的人，对已知的组件的存在的安全漏洞做了一个共享数据库，这个插件可以对依赖的版本进行扫描，看你的组件有没有不合规的版本。

你如果高兴对于级别配置了Maven编译那么在编译时就会进行依赖检测，

二、使用CLI方式

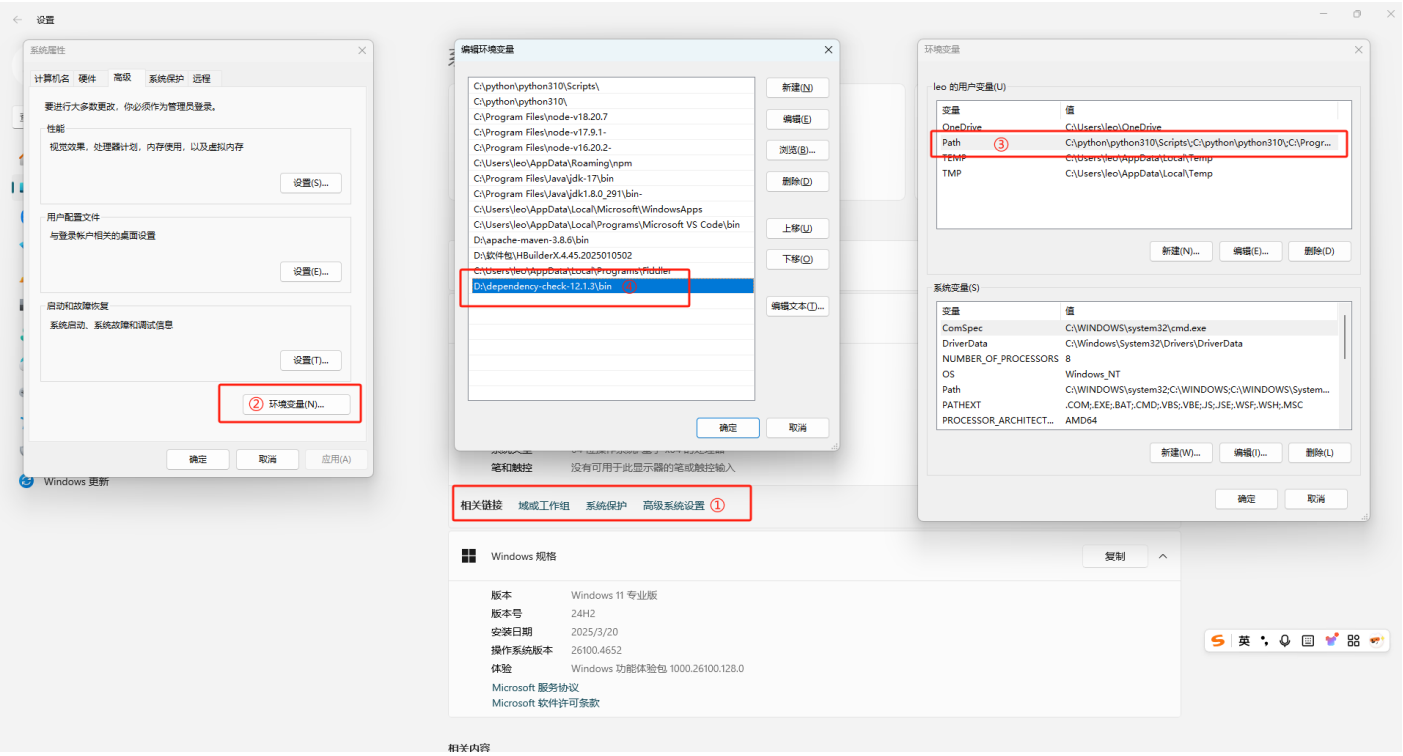
CLI官网：https://dependency-check.github.io/DependencyCheck/dependency-check-cli/index.html

CLI参数：https://dependency-check.github.io/DependencyCheck/dependency-check-cli/arguments.html

扫描之前需要先编译打包: **mvn clean install**

```
# 下载cli版本

https://github.com/dependency-check/DependencyCheck/releases/

# 更新漏洞库
dependency-check --updateonly --nvdDatafeed https://nvdcve.iovhm.com --retireJsUrl
http://nvdcve.iovhm.com/jsrepository.json

# 扫描
dependency-check --noupdate --failOnCVSS 7 --scan "D:\vpclub\park-baiyun\baiyun-back\**\*.jar"

# 如果加入过环境变量，可以进入到项目文件夹执行
# --noupdate 不更新数据库
# --failOnCVSS 7 只扫描高位漏洞
# --format CSV ，默认输出为html，很卡，可以输出为csv
dependency-check --noupdate --failOnCVSS 7 --scan  ./target/*.jar --format CSV

# 输出为csv格式时，主要查看 CVSSv3_BaseScore 列，筛选7和以上的优先修复。或者查看CVSSv3_BaseSeverity 列，优先修复高(HIGH)和严重(CRITICAL)
```

□□□□□□□□bin□□□□□□□□□□□□□□□□□□□dependency-check□□□□□□□□path



□□JAVA 8

□□□□□□□□java 8 □□□□□□□□□□□□□java 8□ □□dependency-check□□□□□□ □□□□□dependency-check.bat □□□□□java□□

```
goto Win9xApp

:Win9xGetScriptDir
set SAVEDIR=%CD%
%0\
cd %0\..\..
set BASEDIR=%CD%
cd %SAVEDIR%
set SAVE_DIR=
goto repoSetup

:WinNTGetScriptDir
for %%i in ("%~dp0..") do set "BASEDIR=%%~fi"

:repoSetup
set REPO=


if "%JAVACMD%"=="" set JAVACMD=C:\Program Files\Java\jdk-17\bin\java

if "%REPO%"=="" set REPO=%BASEDIR%\lib

set CLASSPATH="%BASEDIR%"\plugins\*;"%REPO%"\*

set ENDORSED_DIR=
if NOT "%ENDORSED_DIR%" == "" set CLASSPATH="%BASEDIR%"\%ENDORSED_DIR%\*;%CLASSPATH%

if NOT "%CLASSPATH_PREFIX%" == "" set CLASSPATH=%CLASSPATH_PREFIX%;%CLASSPATH%

@REM Reaching here means variables are defined and arguments have been captured
:endInit
```

□□□mvn□□□

```
failBuildOnCVSS□□□□11□□□□□□□□□□
```

dependency-check-maven

maven https://central.sonatype.com/artifact/org.owasp/dependency-check-maven

maven https://dependency-check.github.io/DependencyCheck/dependency-check-maven/

maven □□□□3.8□□

JDK 8 □□□□□□□10.0.3□□□□□□2023□□□□□□□□□□□□□□□□□CLI□□

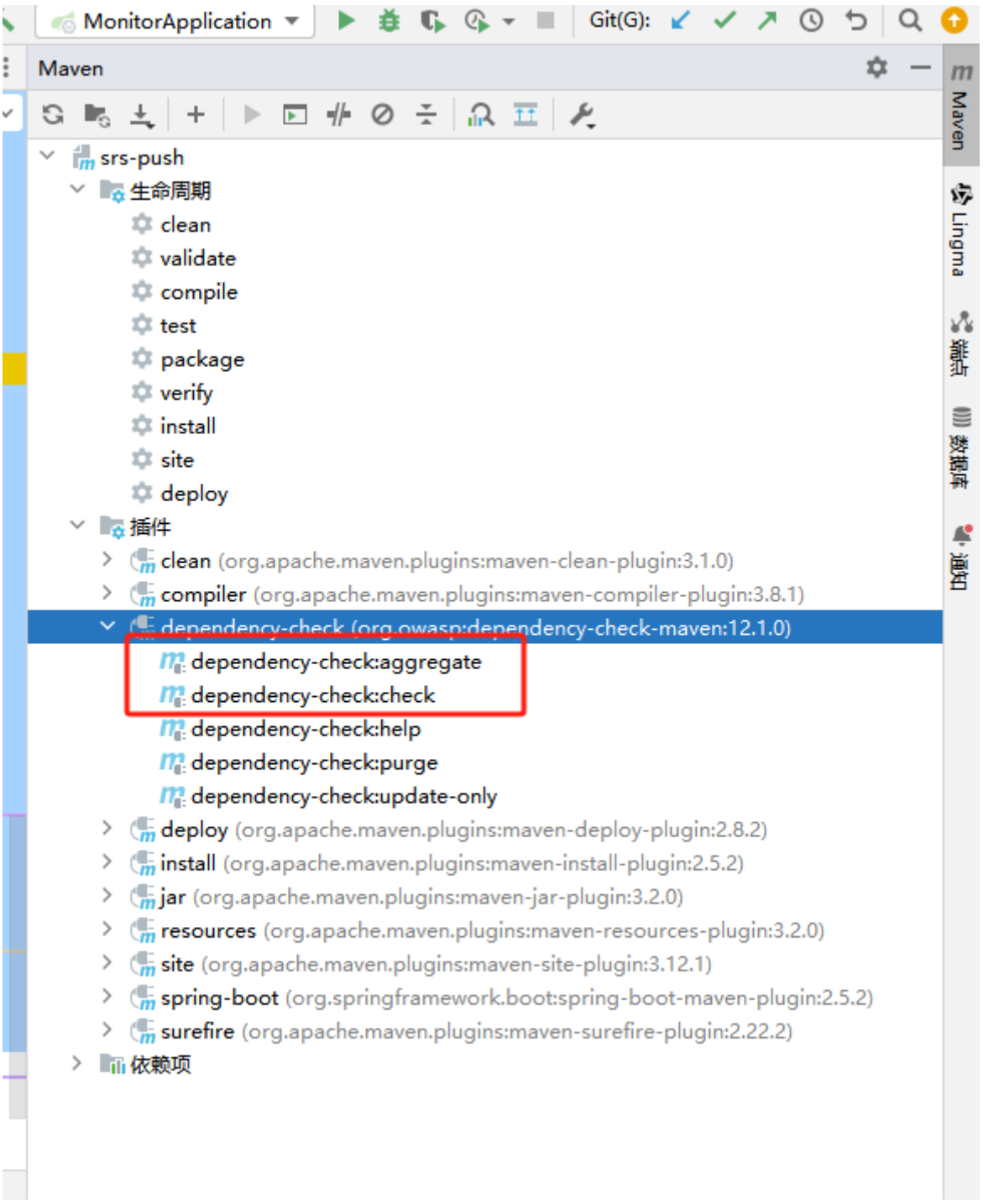
□□mvn□□

```
<build>
    <plugins>
        <plugin>
            <groupId>org.owasp</groupId>
            <artifactId>dependency-check-maven</artifactId>
            <version>12.1.3</version>
            <configuration>
                <!-- 使用美国国家中心的数据库需要的秘钥，如果配置了镜像可以不需要-->
                <nvdApiKey>your_key</nvdApiKey>
                <!-- 手动更新漏洞数据库 -->
                <autoUpdate>false</autoUpdate>
                <!-- nvdcve 漏洞库镜像地址 -->
                <nvdDatafeedUrl>https://nvdcve.iovhm.com</nvdDatafeedUrl>
                <!-- retire.js 漏洞库镜像地址 -->
                <retireJsUrl>http://nvdcve.iovhm.com/jsrepository.json</retireJsUrl>
                <!-- 只扫描风险评分大于等于这个数值的，既高危漏洞 -->
                <failBuildOnCVSS>7</failBuildOnCVSS>
            </configuration>
            <executions>
                <execution>
                    <goals>
                        <goal>check</goal>
                        <goal>update-only</goal>
                        <goal>aggregate</goal>
                    </goals>
                </execution>
            </executions>
        </plugin>
    </plugins>
</build>
```

执行依赖CVE检测

```
# 升级漏洞库
mvn dependency-check:update-only

# 对整个多模块项目（含所有子模块）执行聚合依赖扫描。递归扫描所有子模块的依赖，合并为一个统一报告。多模块项目，想一次性检查所有模块的依赖。
```

```
mvn dependency-check:aggregate

# 或者 Maven 命令 检查项目中的依赖项是否存在已知的漏洞
mvn dependency-check:check
```



```
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Created CPE Index (4 seconds)
[INFO] Finished CPE Analyzer (5 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Sonatype OSS Index Analyzer (0 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Known Exploited Vulnerability Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Finished Unused Suppression Rule Analyzer (0 seconds)
[INFO] Analysis Complete (9 seconds)
[INFO] Writing HTML report to: D:\iovhm\qq829cn\ossrs\nvr\easynvr-api\target\dependency-check-report.html
[WARNING]

One or more dependencies were identified with known vulnerabilities in srs-push:

jackson-core-2.12.3.jar (pkg:maven/com.fasterxml.jackson.core/jackson-core@2.12.3, cpe:2.3:a:fasterxml:jackson-modules-java8:
jackson-databind-2.12.3.jar (pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.12.3, cpe:2.3:a:fasterxml:jackson-databi
```

查看扫描报告

我这个项目啥也没有，就检查出这么多问题

Summary

点击列头可以排序

Display: Showing All Dependencies (click to show less)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence↑	Evidence Count
snakeyaml-1.28.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.28:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.28	CRITICAL	7	Highest	44
spring-boot-2.5.2.jar	cpe:2.3:a:vmware:spring_boot:2.5.2:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.5.2	CRITICAL	2	Highest	38
spring-boot-starter-web-2.5.2.jar	cpe:2.3:a:vmware:spring_boot:2.5.2:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:2.5.2:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.5.2	CRITICAL	2	Highest	36
spring-context-5.3.8.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.8:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-context@5.3.8	CRITICAL*	14	Highest	35
spring-core-5.3.8.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.8:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.8	CRITICAL*	13	Highest	37
spring-web-5.3.8.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.3.8:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.3.8	CRITICAL*	19	Highest	35
spring-webmvc-5.3.8.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.8:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.3.8:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.3.8	CRITICAL*	14	Highest	37
tomcat-embed-core-9.0.48.jar	cpe:2.3:a:apache:tomcat:9.0.48:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.48:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.48	CRITICAL*	27	Highest	65
jackson-databind-2.12.3.jar	cpe:2.3:a:fasterxml:jackson-databind:2.12.3:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.12.3:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.12.3	HIGH	5	Highest	41
logback-classic-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-classic@1.2.3	HIGH	2	Highest	31
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-core@1.2.3	HIGH	4	Highest	31
hutool-all-5.8.25.jar	cpe:2.3:a:hutool:hutool:5.8.25:*:*:*:*:*:*:*	pkg:maven/cn.hutool/hutool-all@5.8.25		0	Highest	29
jul-to-slf4j-1.7.31.jar		pkg:maven/org.slf4j/jul-to-slf4j@1.7.31		0		26
log4j-api-2.14.1.jar	cpe:2.3:a:apache:log4j:2.14.1:*:*:*:*:*:*:*	pkg:maven/org.apache.logging.log4j/log4j-api@2.14.1		0	Highest	42
log4j-to-slf4j-2.14.1.jar		pkg:maven/org.apache.logging.log4j/log4j-to-slf4j@2.14.1		0		40
lombok-1.18.22.jar		pkg:maven/org.projectlombok/lombok@1.18.22		0		36
slf4j-api-1.7.31.jar		pkg:maven/org.slf4j/slf4j-api@1.7.31		0		27

高和以上的必须修复

四、漏洞库代理

在没有修改配置的情况下，插件使用美国国家数据库，很慢、半个小时都搞不完，这个时候你需要一个漏洞数据库镜像。

如果你不具备自己搭建漏洞镜像数据库的条件，可以到美国国家数据库申请一个key，会稍微快点，但是还是很慢。

美国国家数据库API_KEY申请：https://nvd.nist.gov/developers/request-an-api-key

https://dependency-check.github.io/DependencyCheck/data/mirrornvd.html

https://github.com/jeremylong/open-vulnerability-cli

```
version: "3"
services:
  open-vulnerability-cli:
    image: harbor.iovhm.com/hub/jeremylong/open-vulnerability-data-mirror:v9.0.0
    container_name: open-vulnerability-cli
    restart: always
    privileged: true
    ports:
      - 8089:80
    environment:
      - TZ=Asia/Shanghai
      - NVD_API_KEY=<your_key>    # 
    volumes:
      - ./cache:/usr/local/apache2/htdocs

# 
# docker exec -it open-vulnerability-cli /bin/bash

# 
# /mirror.sh

# jsrepository.json , /cache
# wget
https://raw.githubusercontent.com/Retirejs/retire.js/master/repository/jsrepository.json
```

mvn

```
                <configuration>
                    <!-- 
                    <nvdApiKey>your_key</nvdApiKey>
                    <!--  -->
                    <autoUpdate>false</autoUpdate>
```

```
            <!-- nvdcve □□□□□□□ -->
            <nvdDatafeedUrl>https://nvdcve.iovhm.com</nvdDatafeedUrl>
            <!-- retire.js □□□□□□□ -->
            <retireJsUrl>http://nvdcve.iovhm.com/jsrepository.json</retireJsUrl>
            <!-- □□□□□□□□□□□□□□□□□□□□□□□□ -->
            <failBuildOnCVSS>7</failBuildOnCVSS>
        </configuration>
```

□□□□□

https://sonatype.github.io/ossindex-maven/maven-plugin/

```
mvn org.sonatype.ossindex.maven:ossindex-maven-plugin:audit -f pom.xml

mvn org.sonatype.ossindex.maven:ossindex-maven-plugin:audit-aggregate -f pom.xml
```

□□□ #47
□ □□□ □□□ 17 □□ 2025 05:49:11
□ □□□ □□□ 29 □□ 2026 16:40:23