Spring4Shell
A Deep Dive

whoami

- Pedro Ribeiro | ex-aws (https://pedroribeiro.io/)
- Sr. Software Engineer @ jumo.world (**we're hiring**)
- Open source contributor
- CTF enthusiast
- Heavy metal head

Agenda

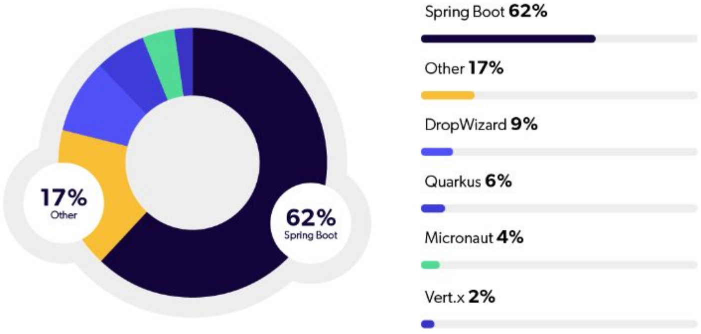
- Overview
- Spring Framework
- Exploitation Requirements
- Deep Dive
- Learnings

Overview

- RCE vulnerability in the Spring Framework (spring-beans package)
- Leaked out ahead of CVE publication
- CVE added on March 31st: CVE-2022-22965
- Not to be confused with the Spring Cloud Functions vulnerability

Spring Framework

- Provides a programming and configuration model for JVM-based applications
- At the heart are the modules of the core container, including a configuration model and a dependency injection mechanism
- Provides foundational support for different application architectures including messaging, transactional data, persistence and web
- Widely used to build web applications
- Open Source



Source: 2021 Java Developer Productivity Report - Most Popular Java Application Frameworks

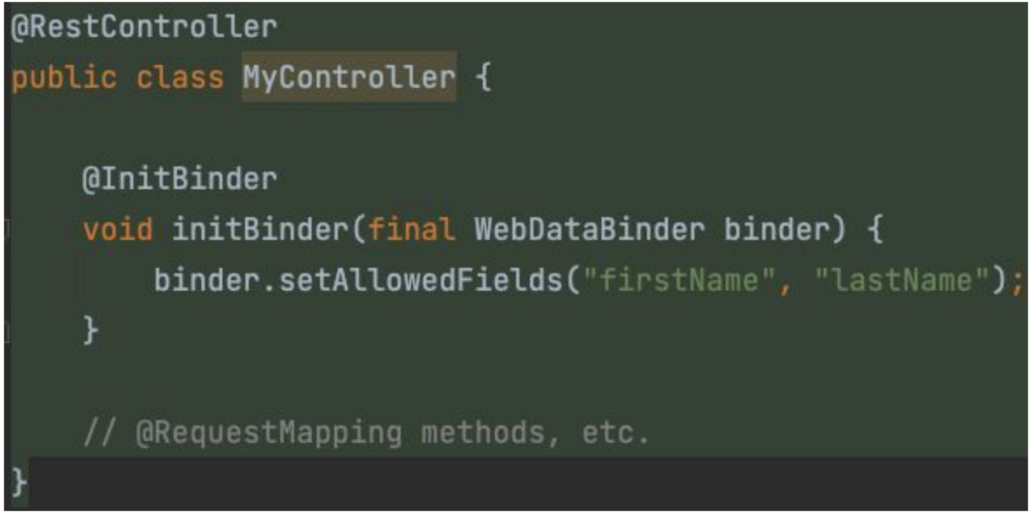
Exploitation requirements

- JDK 9+
- Vulnerable version of the Spring Framework (<5.2 | 5.2.0-19 | 5.3.0-17)
- A dependency on the Spring Web MVC and/or Spring WebFlux (transitively affected from Spring Beans)
- Packaged as a WAR and deployed on a standalone Servlet container (Deployments using an embedded Servlet container or reactive web server are not affected)
- Using DataBinder to populate controller method parameters
- Does not relate to @RequestBody method parameters (e.g. JSON deserialization).

Demo

Lessons learned

- Keep your dependencies updated
- Use a dedicated model object for each data binding use-case
- Use setAllowedFields() method on WebDataBinder otherwise



```java
@RestController
public class MyController {

    @InitBinder
    void initBinder(final WebDataBinder binder) {
        binder.setAllowedFields("firstName", "lastName");
    }

    // @RequestMapping methods, etc.
}
```

Thank you

Questions?