Assignment 1
Research of a security vulnerability

CVE - 2022-22965
Spring4Shell

David Amorim - 112610
Francisca Silva - 112841
Gabriel Santos - 113682
Henrique Freitas - 114990

TABLE OF CONTENTS

01.

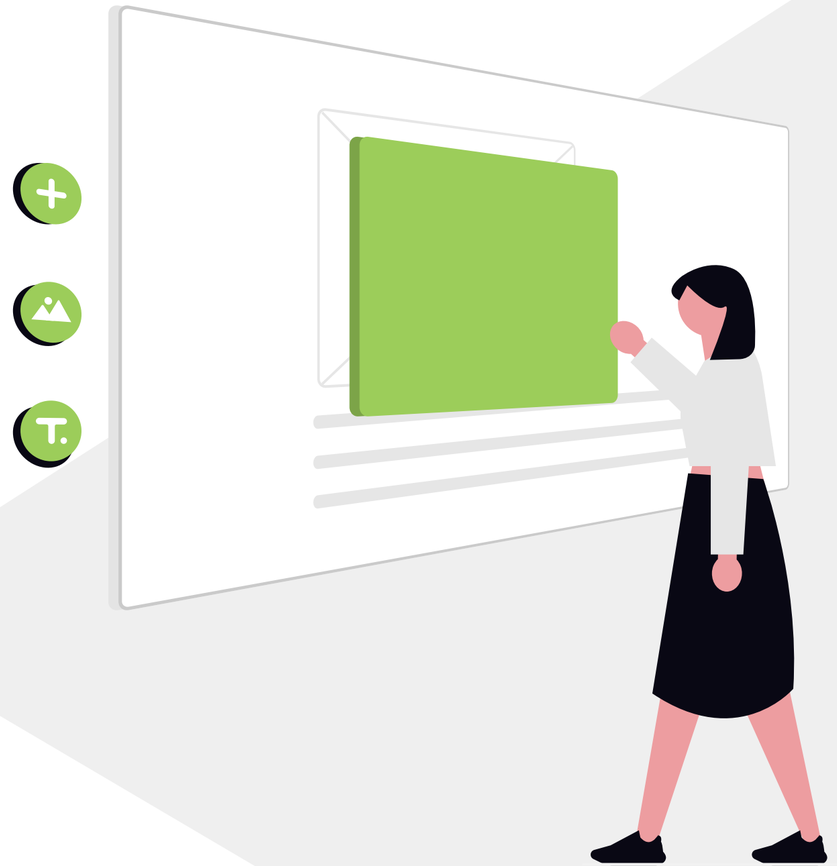
Product

Spring Framework

The Spring Framework is an open-source framework for building web applications in Java.

Provides a comprehensive programming and configuration model for modern Java-based enterprise applications.

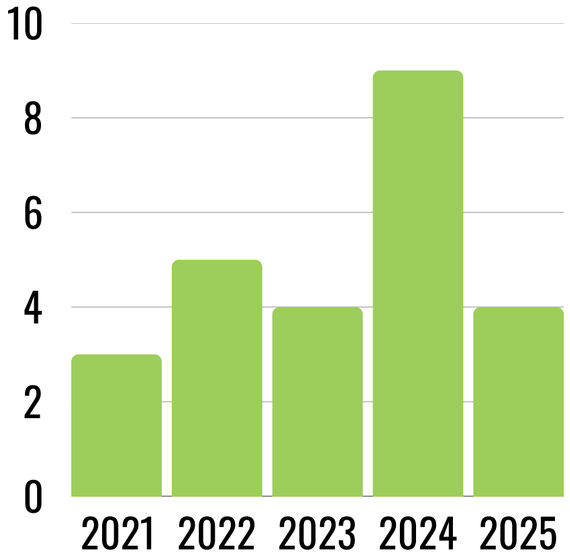
Spring Framework is part of the Spring ecosystem, which comprises other components for cloud, data, and security, among others.



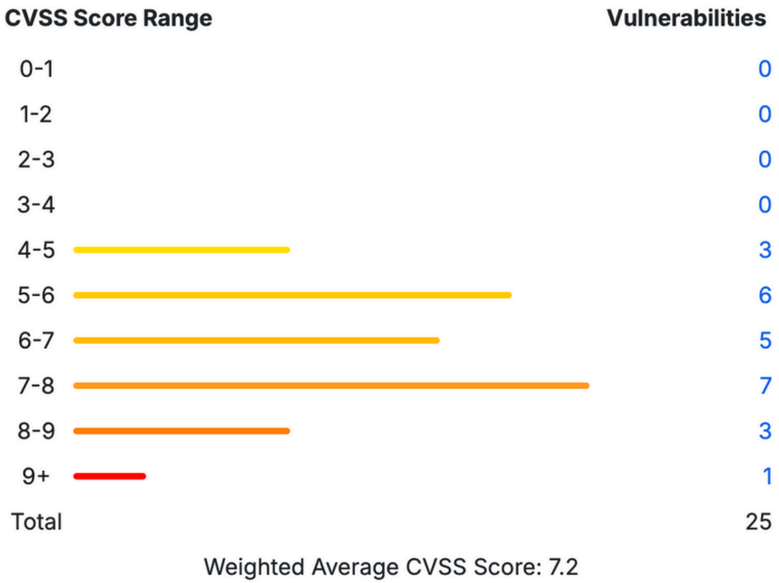
02.

Security Record

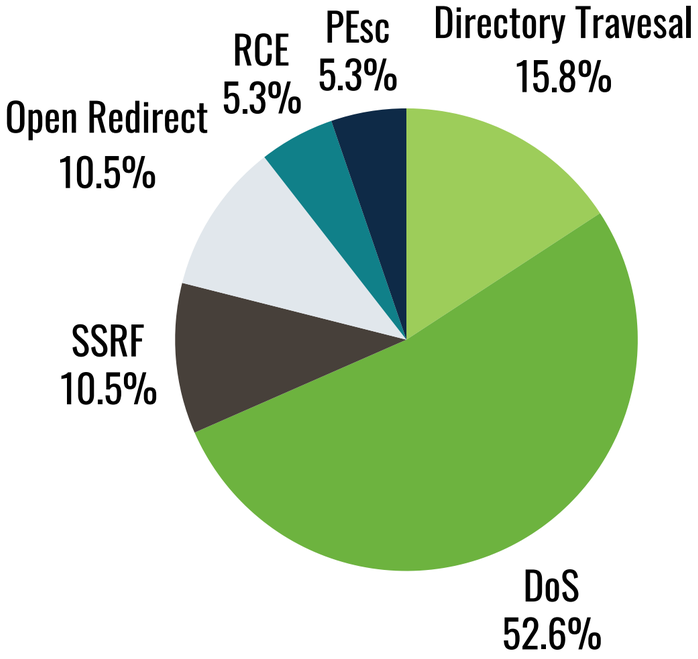
Vulnerabilities in the last years



Number of CVE's/Year



CVSS Scores



Vulnerability Category

03.

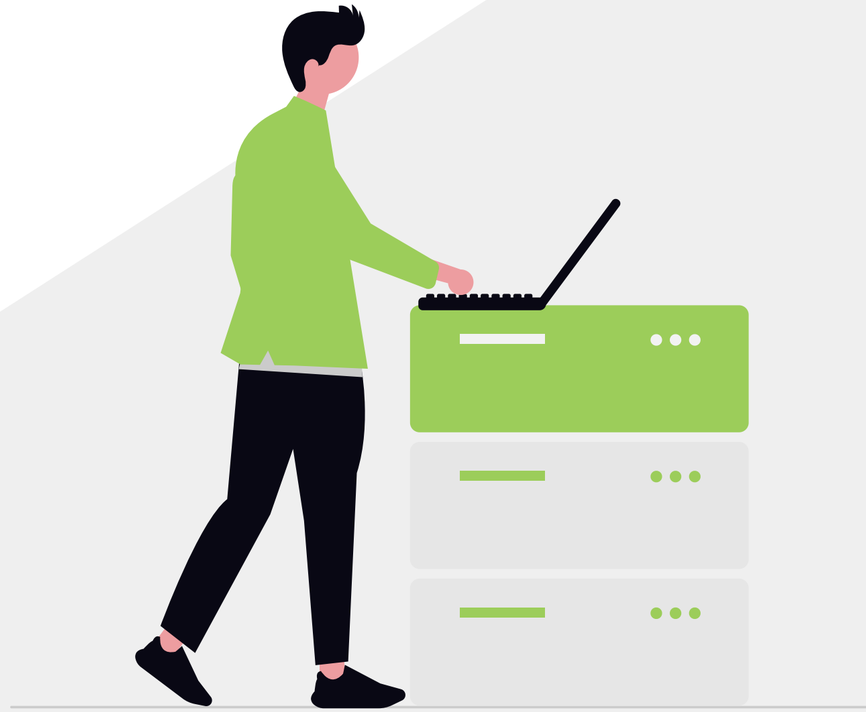
Spring4Shell

Previous Vulnerabilities

In June 2010, a CVE was published for the Spring framework.

Tomcat uses its own class loader for its web applications. This class loader uses an array of URL's to retrieve resources.

Overwriting one of the URLs with a URL to a remote JAR file would cause Tomcat to subsequently load the JAR from an attacker-controlled location.



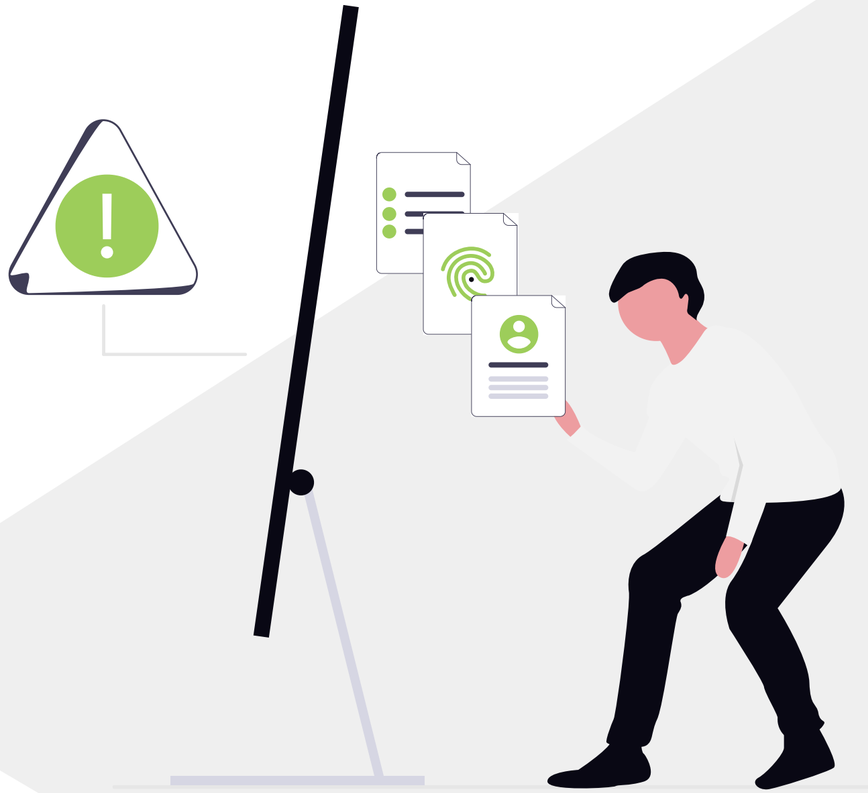
What was the vulnerability?

The attacker sends a request with a crafted parameter name, and that object properties will be traversed.

The data binder will accept and apply those properties.

The attacker then requests the dropped file and executes arbirtary code on the server.

CVSS v.3.1 : 9.8 CRITICAL

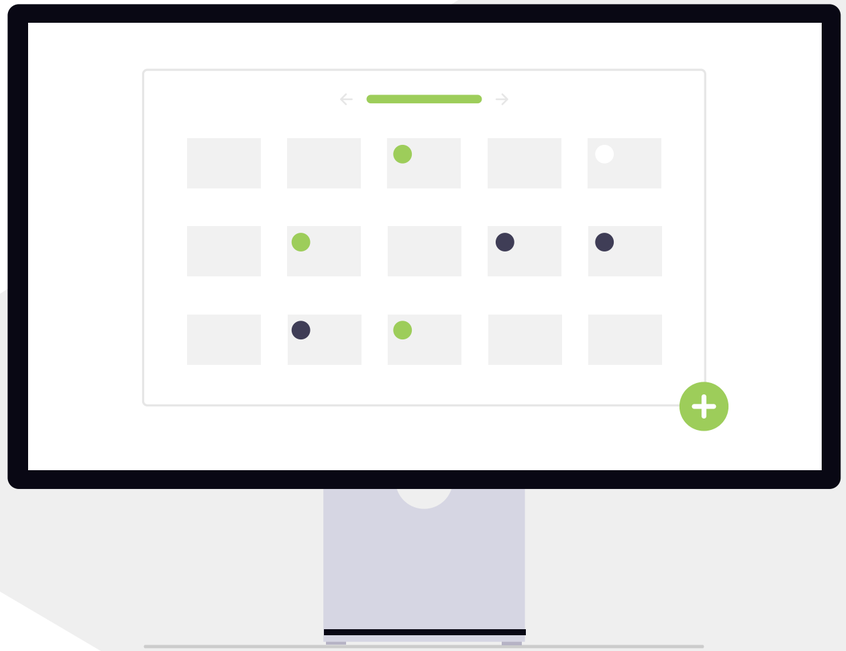


Report Date

Discovery date: March 29th 2022
This vulnerability was responsibly reported to VMware by codeplutos, meizjm3i of AntGroup FG Security Lab.

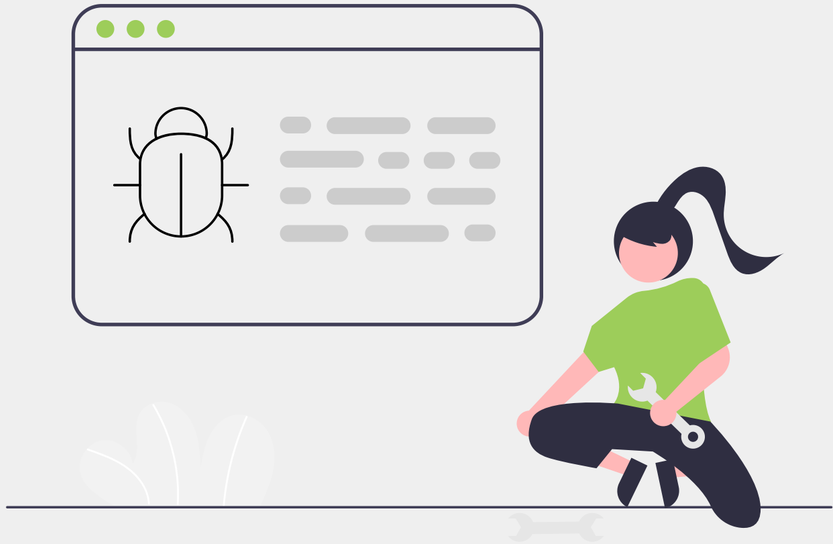
Official Spring Announcement & CVE assignment:

March 31st 2022



When/How was it fixed?

- Spring released fixed Framework versions 5.3.18 and 5.2.20 on March 31, 2022, which changed binding rules to deny dangerous property access and tightened defaults.
- Spring also published guidance and workarounds.
- Apache Tomcat released fixed versions 10.0.20, 9.0.62, and 8.5.78 disabling WebappClassLoaderBase.getResources()



When/How was it fixed?

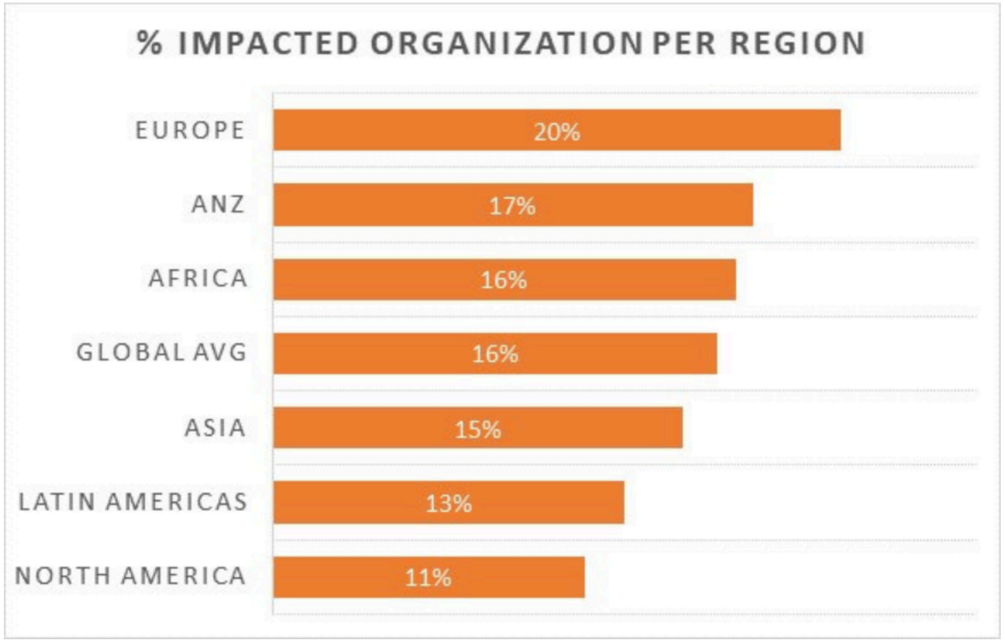
```java
@ControllerAdvice
public class GlobalBindingConfig {

    @InitBinder
    public void initBinder(WebDataBinder binder) {
        // Disallow binding to 'class' and nested properties under it
        binder.setDisallowedFields("class.*");
    }
}
```

Vendors

VMware	Their Cloud and Spring based components	They released patches and workarounds
Atlassian	Atlassian Connect Spring Boot (ASCB)	They said they used a vulnerable version and they were investigating the impact
Cisco	Multiple products / Network devices	Cisco released advisories, investigating possible vulnerabilities in it's products
Red Hat	Enterprise Java	Red Hat indicated that products such as JBoss might be affected
VMware (Blockchain)	VMware Blockchain nodes	VMware's knowledge base noted that for their blockchain product lines, some node versions required fixes or scans, though they claimed in some versions the vulnerability was not exploitable

OVERALL IMPACT



Source: https://blog.checkpoint.com/security/16-of-organizations-worldwide-impacted-by-spring4shell-zero-day-vulnerability-exploitation-attempts-since-outbreak/

04.

Demo

THANKS

DO YOU HAVE ANY QUESTIONS?