CVE-2022-22965, Spring4Shell

▼ 취약점

- A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it. - HackerOne, NVD

  JDK 9+에서 실행되는 Spring MVC 또는 Spring WebFlux 애플리케이션은 데이터 바인딩을 통해 원격 코드 실행(RCE)에 취약할 수 있다. 특정 익스플로잇은 애플리케이션이 Tomcat에서 WAR 배포로 실행되어야 한다. 애플리케이션이 jar 형식의 Spring Boot 실행 파일 즉, 기본값으로 배포되는 경우 익스플로잇에 취약하지 않다. 그러나 이 취약점의 특성은 더 일반적이며, 이를 악용하는 다른 방법이 있을 수 있다.

- Spring Core 프레임워크에서 특정 조건 하에 Remote Code Execution이 가능한 취약점으로, Spring 프레임워크가 매개변수를 바인딩하는 과정에서 class 객체가 노출되어 발생한다.

- 공격자는 해당 class 객체의 자식 객체인 class.module.classLoader에 웹 매개변수를 통해 접근할 수 있으며, 로깅 관련 클래스인 AccessLogValue를 이용하여 웹 쉘 코드를 업로드한 후, 명령어를 실행할 수 있다.

▼ Mechanism

[피해자]

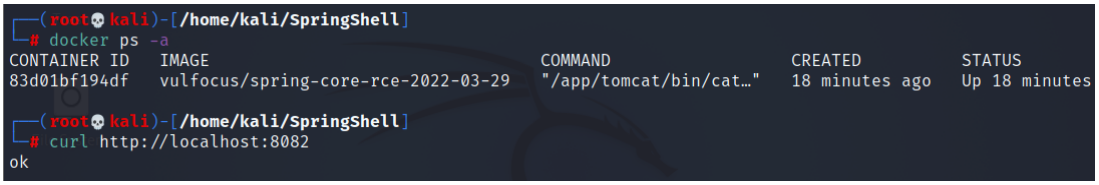
1. 웹 어플리케이션 이용자가 매개변수를 사용하는 페이지에 접근한다.

2. 어플리케이션은 요청 매개변수를 POJO(Plain Old Java Object, Java로 생성하는 순수한 객체)에 바인딩하기 위해 getCachedIntrospectionResults 라는 메서드를 호출한 후 캐시의 Object 속성을 가져온다. 이때 POJO는 @RequestBody annotation이 적용되어 있지 않아야 한다.
3. 반환된 Object에는 class가 포함되어 있어 사용자는 class 객체를 원격에서 사용할 수 있게 된다.
4. 이용자는 요청 패킷 매개변수에 class의 자식 객체인 class.module.classLoader와 로깅 관련 클래스를 입력, 전송하여 객체를 이용할 수 있다.
   Spring Core 프레임워크에서 필터링하는 객체를 우회하여 사용해야 한다.

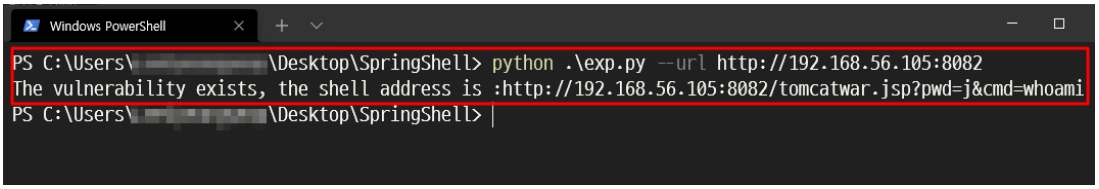
[공격자]

1. 취약한 도커 이미지 실행

```
docker run -d =p 8082:8080 --name springrce -it vulfocus/spring-core-rce-2022-03-29
```

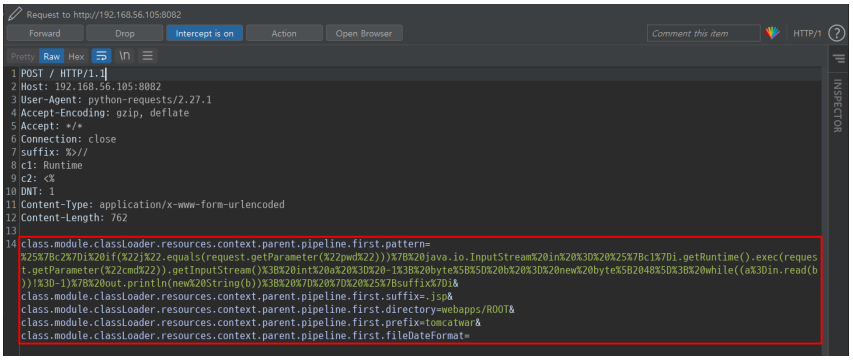


2. POC 실행
   POC 실행 시 취약한 서버에 웹쉘이 생성된다.



   POC 요청 패킷에 매개변수 class의 로깅 관련 객체가 사용되는 것을 확인할 수 있다.

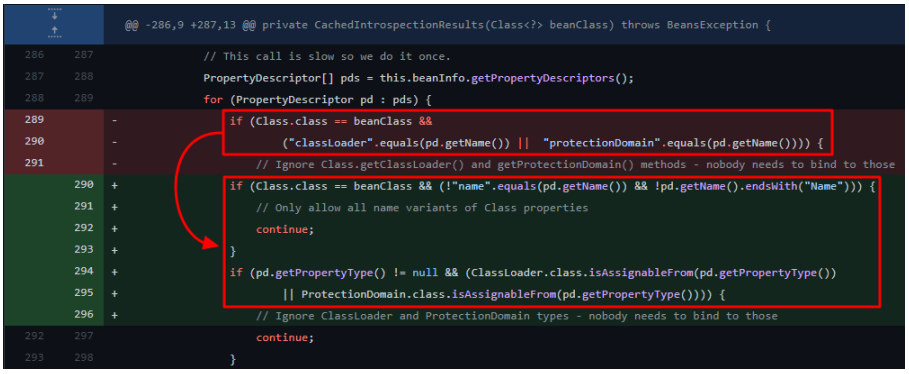
   class.module.classLoader.resources.context.parent.pipeline.first.pattern 매개변수에 웹 쉘의 코드를 담고 있다.



▼ 대응 방안

- 패치 전에는 class의 자식 객체에 대한 직접 접근을 필터링하기 위해 CachedIntrospectionResults.java에서 class.classLoader 및 class.protectionDomain을 필터링 하였으나 class.module.classLoader를 사용하여 우회 가능하였음.

- Spring 개발자에 의해 패치되어 아래와 같이 수정됨.



▼ 참고자료

- https://hackerone.com/hacktivity/cve_discovery?id=CVE-2022-22965
- https://nvd.nist.gov/vuln/detail/cve-2022-22965
- https://velog.io/@thelm3716/spring4shell-CVE-2022-22965
- https://github.com/spring-projects/spring-framework/commit/002546b3e4b8d791ea6acccb81eb3168f51abb15
- https://github.com/lunasec-io/lunasec/blob/master/docs/blog/2022-03-30-spring-core-rce.mdx#who-is-impacted