Vulnerability Report

Project Name: Book Shop

Author: Le Hoang Phuc

Exported On: 2024-06-30:01:28:58

Ecosystem: Maven

Amount: 27

No.	Database Id	Package Name	Version	Summary	Fix Version	Severity	Score
1	GHSA-493p-pfq6-5258	net.minidev:json-smart	2.4.8	json-smart Uncontrolled Recursion vulnerabilty	2.4.9	High	7.5
2	GHSA-x873-6rgc-94jc	org.springframework.security:spring-security-core	6.0.1	Spring Security logout not clearing security context	6.0.3	Medium	6.3
3	GHSA-f3jh-qvm4-mg39	org.springframework.security:spring-security-core	6.0.1	Erroneous authentication pass in Spring Security	6.1.8	High	8.2
4	GHSA-vmq6-5m68-f53m	ch.qos.logback:logback-classic	1.4.5	logback serialization vulnerability	1.4.12	High	7.1
5	GHSA-q3mw-pvr8-9ggc	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	Apache Tomcat Open Redirect vulnerability	10.1.13	Medium	6.1
6	GHSA-r6j3-px5g-cq3x	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	Apache Tomcat Improper Input Validation vulnerability	10.1.14	Medium	5.3
7	GHSA-fccv-jmmp-qg76	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	Apache Tomcat Improper Input Validation vulnerability	10.1.16	High	7.5
8	GHSA-qppj-fm5r-hxr3	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	HTTP/2 Stream Cancellation Attack	10.1.14	Medium	5.3

9	GHSA-7w75-32cg-r6g2	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	Apache Tomcat Denial of Service due to improper input validation vulnerability for HTTP/2 requests	10.1.19		
10	GHSA-cx6h-86xw-9x34	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	Apache Tomcat - Fix for CVE-2023-24998 was incomplete	10.1.8	High	7.5
11	GHSA-g8pj-r55q-5c2v	org.apache.tomcat.embed:tomcat-embed-core	10.1.5	Apache Tomcat Incomplete Cleanup vulnerability	10.1.14	Medium	5.3
12	GHSA-2wrp-6fg6-hmc5	org.springframework:spring-web	6.0.4	Spring Framework URL Parsing with Host Validation	6.0.19	High	8.1
13	GHSA-ccgv-vj62-xf9h	org.springframework:spring-web	6.0.4	Spring Web vulnerable to Open Redirect or Server Side Request Forgery	6.0.17	High	8.1
14	GHSA-hgjh-9rj2-g67j	org.springframework:spring-web	6.0.4	Spring Framework URL Parsing with Host Validation Vulnerability	6.0.18	High	8.1
15	GHSA-3h6f-g5f3-gc4w	org.springframework.security:spring-security-config	6.0.1	Access Control Bypass in Spring Security	6.0.5	Critical	9.1
16	GHSA-4vpr-xfrp-cj64	org.springframework.security:spring-security-config	6.0.1	Spring Security's authorization rules can be misconfigured when using multiple servlets	6.0.5	High	7.3
17	GHSA-564r-hj7v-mcr5	org.springframework:spring-expression	6.0.4	Spring Framework vulnerable to denial of service via specially crafted SpEL expression	6.0.7	Medium	6.5
18	GHSA-wxqc-pxw9-g2p8	org.springframework:spring-expression	6.0.4	Spring Framework vulnerable to denial of service	6.0.8	High	7.5
19	GHSA-xf96-w227-r7c4	org.springframework.boot:spring-boot-autoconfigure	3.0.2	Spring Boot Welcome Page Denial of Service	3.0.7	High	7.5
20	GHSA-chfm-68vv-pvw5	org.xmlunit:xmlunit-core	2.9.1	XMLUnit for Java has Insecure Defaults when Processing XSLT Stylesheets	2.10.0		

21	GHSA-v682-8vv8-vpwr	org.apache.tomcat.embed:tomcat-embed-websocket	10.1.5	Denial of Service via incomplete cleanup vulnerability in Apache Tomcat	10.1.19		
22	GHSA-mjmj-j48q-9wg2	org.yaml:snakeyaml	1.33	SnakeYaml Constructor Deserialization Remote Code Execution	2.0	High	8.3
23	GHSA-jjfh-589g-3hjx	org.springframework.boot:spring-boot	3.0.2	Spring Boot denial of service vulnerability	3.0.13	Medium	6.5
24	GHSA-gvpg-vgmx-xg6w	com.nimbusds:nimbus-jose-jwt	9.24.4	Denial of Service in Connect2id Nimbus JOSE+JWT	9.37.2		
25	GHSA-pfh2-hfmq-phg5	com.jayway.jsonpath:json-path	2.7.0	json-path Out-of-bounds Write vulnerability	2.9.0	Medium	5.3
26	GHSA-vmq6-5m68-f53m	ch.qos.logback:logback-core	1.4.5	logback serialization vulnerability	1.4.12	High	7.1
27	GHSA-v94h-hvhg-mf9h	org.springframework:spring-webmvc	6.0.4	Spring Framework vulnerable to denial of service	6.0.14	High	7.5