~~~~~~~~~~~~~~~ Summary ~~~~~~~~~~~~~~~
Scan Score - 0
Low - 0
Medium - 10
High - 6
Critical - 7

~~~~~~~~~~~~~~~ Vulnerability 1 ~~~~~~~~~~~~~~~
ID - CVE-2014-0054
Artifact - spring-boot-starter-web 3.2.4
Group - org.springframework.boot
Description - The Jaxb2RootElementHttpMessageConverter in Spring MVC in Spring Framework before 3.2.8 and 4.0.0 before 4.0.2 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4152, CVE-2013-7315, and CVE-2013-6429.
Severity - Medium
CVSS - 6.8
Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative
Discovery Date - 17/04/2014
Resource - https://nvd.nist.gov/vuln/detail/CVE-2014-0054
Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 2 ~~~~~~~~~~~~~~~
ID - CVE-2015-3192
Artifact - spring-boot-starter-web 3.2.4
Group - org.springframework.boot
Description - Pivotal Spring Framework before 3.2.14 and 4.x before 4.1.7 do not properly process inline DTD declarations when DTD is not entirely disabled, which allows remote attackers to cause a denial of service (memory consumption and out-of-memory errors) via a crafted XML file.
Severity - Medium
CVSS - 5.5
Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative
Discovery Date - 12/07/2016
Resource - https://nvd.nist.gov/vuln/detail/CVE-2015-3192
Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 3 ~~~~~~~~~~~~~~~
ID - CVE-2016-9878
Artifact - spring-boot-starter-web 3.2.4
Group - org.springframework.boot
Description - An issue was discovered in Pivotal Spring Framework before 3.2.18, 4.2.x before 4.2.9, and 4.3.x before 4.3.5. Paths provided to the ResourceServlet were not properly sanitized and as a result exposed to directory traversal attacks.
Severity - High
CVSS - 7.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative
Discovery Date - 29/12/2016
Resource - https://nvd.nist.gov/vuln/detail/CVE-2016-9878
Days To Remediate - 30

~~~~~~~~~~~~~~~ Vulnerability 4 ~~~~~~~~~~~~~~~

ID - CVE-2014-0225

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - When processing user provided XML documents, the Spring Framework 4.0.0 to 4.0.4, 3.0.0 to 3.2.8, and possibly earlier unsupported versions did not disable by default the resolution of URI references in a DTD declaration. This enabled an XXE attack.

Severity - High

CVSS - 8.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/05/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2014-0225

Days To Remediate - 30

~~~~~~~~~~~~~~~ Vulnerability 5 ~~~~~~~~~~~~~~~

ID - CVE-2015-5211

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Under some situations, the Spring Framework 4.2.0 to 4.2.1, 4.0.0 to 4.1.7, 3.2.0 to 3.2.14 and older unsupported versions is vulnerable to a Reflected File Download (RFD) attack. The attack involves a malicious user crafting a URL with a batch script extension that results in the response being downloaded rather than rendered and also includes some input reflected in the response.

Severity - Critical

CVSS - 9.6

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/05/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2015-5211

Days To Remediate - 15

~~~~~~~~~~~~~~~ Vulnerability 6 ~~~~~~~~~~~~~~~

ID - CVE-2016-5007

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Both Spring Security 3.2.x, 4.0.x, 4.1.0 and the Spring Framework 3.2.x, 4.0.x, 4.1.x, 4.2.x rely on URL pattern mappings for authorization and for mapping requests to controllers respectively. Differences in the strictness of the pattern matching mechanisms, for example with regards to space trimming in path segments, can lead Spring Security to not recognize certain paths as not protected that are in fact mapped to Spring MVC controllers that should be protected. The problem is compounded by the fact that the Spring Framework provides richer features with regards to pattern matching as well as by the fact that pattern matching in each Spring Security and the Spring Framework can easily be customized creating additional differences.

Severity - High

CVSS - 7.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/05/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2016-5007

Days To Remediate - 30

~~~~~~~~~~~~~~~ Vulnerability 7 ~~~~~~~~~~~~~~~

ID - CVE-2018-1270

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack.

Severity - Critical

CVSS - 9.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 06/04/2018

Resource - https://nvd.nist.gov/vuln/detail/CVE-2018-1270

Days To Remediate - 15

~~~~~~~~~~~~~~~ Vulnerability 8 ~~~~~~~~~~~~~~~

ID - CVE-2018-1257

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Spring Framework, versions 5.0.x prior to 5.0.6, versions 4.3.x prior to 4.3.17, and older unsupported versions allows applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a regular expression, denial of service attack.

Severity - Medium

CVSS - 6.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 11/05/2018

Resource - https://nvd.nist.gov/vuln/detail/CVE-2018-1257

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 9 ~~~~~~~~~~~~~~~

ID - CVE-2018-11039

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Spring Framework (versions 5.0.x prior to 5.0.7, versions 4.3.x prior to 4.3.18, and older unsupported versions) allow web applications to change the HTTP request method to any HTTP method (including TRACE) using the HiddenHttpMethodFilter in Spring MVC. If an application has a pre-existing XSS vulnerability, a malicious user (or attacker) can use this filter to escalate to an XST (Cross Site Tracing) attack.

Severity - Medium

CVSS - 5.9

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/06/2018

Resource - https://nvd.nist.gov/vuln/detail/CVE-2018-11039

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 10 ~~~~~~~~~~~~~~~

ID - CVE-2018-11040

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Spring Framework, versions 5.0.x prior to 5.0.7 and 4.3.x prior to 4.3.18 and older unsupported versions, allows web applications to enable cross-domain requests via JSONP (JSON with Padding) through AbstractJsonpResponseBodyAdvice for REST controllers and MappingJackson2JsonView for browser requests. Both are not enabled by default in Spring Framework nor Spring Boot, however, when MappingJackson2JsonView is configured in an application, JSONP support is automatically ready to use through the "jsonp" and "callback" JSONP parameters, enabling cross-domain requests.

Severity - High

CVSS - 7.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/06/2018

Resource - https://nvd.nist.gov/vuln/detail/CVE-2018-11040

Days To Remediate - 30

~~~~~~~~~~~~~~~ Vulnerability 11 ~~~~~~~~~~~~~~~

ID - CVE-2016-1000027

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

Severity - Critical

CVSS - 9.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 02/01/2020

Resource - https://nvd.nist.gov/vuln/detail/CVE-2016-1000027

Days To Remediate - 15

~~~~~~~~~~~~~~~ Vulnerability 12 ~~~~~~~~~~~~~~~

ID - CVE-2020-5421

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

Severity - Medium

CVSS - 6.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 19/09/2020

Resource - https://nvd.nist.gov/vuln/detail/CVE-2020-5421

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 13 ~~~~~~~~~~~~~~~

ID - CVE-2022-22950

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - n Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

Severity - Medium

CVSS - 6.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 01/04/2022

Resource - https://nvd.nist.gov/vuln/detail/CVE-2022-22950

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 14 ~~~~~~~~~~~~~~~

ID - CVE-2022-22965

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - 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.

Severity - Critical

CVSS - 9.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 01/04/2022

Resource - https://nvd.nist.gov/vuln/detail/CVE-2022-22965

Days To Remediate - 15

~~~~~~~~~~~~~~~ Vulnerability 15 ~~~~~~~~~~~~~~~

ID - CVE-2022-22968

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

Severity - Medium

CVSS - 5.3

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 14/04/2022

Resource - https://nvd.nist.gov/vuln/detail/CVE-2022-22968

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 16 ~~~~~~~~~~~~~~~

ID - CVE-2022-22970

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

Severity - Medium

CVSS - 5.3

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 12/05/2022

Resource - https://nvd.nist.gov/vuln/detail/CVE-2022-22970

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 17 ~~~~~~~~~~~~~~~

ID - CVE-2023-20861

Artifact - spring-boot-starter-web 3.2.4

Group - org.springframework.boot

Description - In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

Severity - Medium

CVSS - 6.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 23/03/2023

Resource - https://nvd.nist.gov/vuln/detail/CVE-2023-20861

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 18 ~~~~~~~~~~~~~~~

ID - CVE-2016-9879

Artifact - spring-boot-starter-security 3.2.4

Group - org.springframework.boot

Description - An issue was discovered in Pivotal Spring Security before 3.2.10, 4.1.x before 4.1.4, and 4.2.x before 4.2.1. Spring Security does not consider URL path parameters when processing security constraints. By adding a URL path parameter with an encoded "/" to a request, an attacker may be able to bypass a security constraint. The root cause of this issue is a lack of clarity regarding the handling of path parameters in the Servlet Specification. Some Servlet containers include path parameters in the value returned for getPathInfo() and some do not. Spring Security uses the value returned by getPathInfo() as part of the process of mapping requests to security constraints. The unexpected presence of path parameters can cause a constraint to be bypassed. Users of Apache Tomcat (all current versions) are not affected by this vulnerability since Tomcat follows the guidance previously provided by the Servlet Expert group and strips path parameters from the value returned by getContextPath(), getServletPath(), and getPathInfo(). Users of other Servlet containers based on Apache Tomcat may or may not be affected depending on whether or not the handling of path parameters has been modified. Users of IBM WebSphere Application Server 8.5.x are known to be affected. Users of other containers that implement the Servlet specification may be affected.

Severity - High

CVSS - 7.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 06/01/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2016-9879

Days To Remediate - 30

~~~~~~~~~~~~~~~ Vulnerability 19 ~~~~~~~~~~~~~~~

ID - CVE-2014-3527

Artifact - spring-boot-starter-security 3.2.4

Group - org.springframework.boot

Description - When using the CAS Proxy ticket authentication from Spring Security 3.1 to 3.2.4 a malicious CAS Service could trick another CAS Service into authenticating a proxy ticket that was not associated. This is due to the fact that the proxy ticket authentication uses the information from the HttpServletRequest which is populated based upon untrusted information within the HTTP request. This means if there are access control restrictions on which CAS services can authenticate to one another, those restrictions can be bypassed. If users are not using CAS Proxy tickets and not basing access control decisions based upon the CAS Service, then there is no impact to users.

Severity - Critical

CVSS - 9.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/05/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2014-3527

Days To Remediate - 15

~~~~~~~~~~~~~~~ Vulnerability 20 ~~~~~~~~~~~~~~~

ID - CVE-2016-5007

Artifact - spring-boot-starter-security 3.2.4

Group - org.springframework.boot

Description - Both Spring Security 3.2.x, 4.0.x, 4.1.0 and the Spring Framework 3.2.x, 4.0.x, 4.1.x, 4.2.x rely on URL pattern mappings for authorization and for mapping requests to controllers respectively. Differences in the strictness of the pattern matching mechanisms, for example with regards to space trimming in path segments, can lead Spring Security to not recognize certain paths as not protected that are in fact mapped to Spring MVC controllers that should be protected. The problem is compounded by the fact that the Spring Framework provides richer features with regards to pattern matching as well as by the fact that pattern matching in each Spring Security and the Spring Framework can easily be customized creating additional differences.

Severity - High

CVSS - 7.5

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 25/05/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2016-5007

Days To Remediate - 30

~~~~~~~~~~~~~~~ Vulnerability 21 ~~~~~~~~~~~~~~~

ID - CVE-2022-22976

Artifact - spring-boot-starter-security 3.2.4

Group - org.springframework.boot

Description - Spring Security versions 5.5.x prior to 5.5.7, 5.6.x prior to 5.6.4, and earlier unsupported versions contain an integer overflow vulnerability. When using the BCrypt class with the maximum work factor (31), the encoder does not perform any salt rounds, due to an integer overflow error. The default settings are not affected by this CVE.

Severity - Medium

CVSS - 5.3

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 19/05/2022

Resource - https://nvd.nist.gov/vuln/detail/CVE-2022-22976

Days To Remediate - 90

~~~~~~~~~~~~~~~ Vulnerability 22 ~~~~~~~~~~~~~~~

ID - CVE-2022-22978

Artifact - spring-boot-starter-security 3.2.4

Group - org.springframework.boot

Description - In spring security versions prior to 5.4.11+, 5.5.7+ , 5.6.4+ and older unsupported versions, RegexRequestMatcher can easily be misconfigured to be bypassed on some servlet containers. Applications using RegexRequestMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass.

Severity - Critical

CVSS - 9.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 19/05/2022

Resource - https://nvd.nist.gov/vuln/detail/CVE-2022-22978

Days To Remediate - 15

~~~~~~~~~~~~~~~ Vulnerability 23 ~~~~~~~~~~~~~~~

ID - CVE-2014-9515

Artifact - dozer 5.5.1

Group - net.sf.dozer

Description - Dozer improperly uses a reflection-based approach to type conversion, which might allow remote attackers to execute arbitrary code via a crafted serialized object.

Severity - Critical

CVSS - 9.8

Remediation Advice - Upgrade dependency, implement mitigation, or use secure alternative

Discovery Date - 29/12/2017

Resource - https://nvd.nist.gov/vuln/detail/CVE-2014-9515

Days To Remediate - 15