**Vulnerability**

1. Spring Boot (2.2.4.RELEASE)

Vulnerability: CVE-2020-5421

Description: Spring Framework, versions 5.2.x prior to 5.2.9 and 5.3.x prior to 5.3 M2, 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 send a specially crafted message to such endpoints and cause a denial of service (DoS).

Severity: High

Status: Fixed in later versions. Update recommended to 5.2.9 or newer in the 5.2 line, or 5.3 M2 or newer in the 5.3 line.

2. Apache BouncyCastle (1.46)

Vulnerability: CVE-2016-1000338

Description: In earlier versions of BouncyCastle before 1.55, DSA does not validate the x parameter associated with the public key, allowing attackers to conduct an invalid curve attack.

Severity: Medium

Status: Update to version 1.55 or later is recommended to mitigate this vulnerability.

3. Spring Boot's Use of Jackson (via spring-boot-starter-web)

Vulnerability: CVE-2017-7525

Description: A deserialization flaw in Jackson's ObjectMapper enables an unauthenticated attacker to perform code execution by submitting maliciously crafted input to an application using the ObjectMapper.

Severity: Critical

Status: It is advisable to upgrade to a Jackson version that has addressed this vulnerability (versions 2.8.11.1, 2.9.5 or later).  
  
**Verification**

All false positive were successfully suppressed and the correct identification of valid dependencies without any misidentified vulnerabilities.