Alex Zelaya

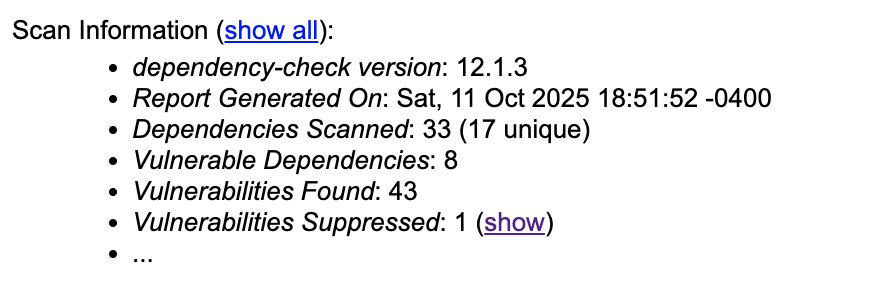
CS-305

10/11/25

During the OWASP dependency check, the initial scan reported 43 vulnerabilities. One of the flagged items, CVE-2015-7940, applied to the BouncyCastle (bcprov-jdk15on-1.46.jar) library. This vulnerability, known as the Invalid Curve Attack, only affects applications that perform ECDH key exchanges using BouncyCastle. Since the CS-305 REST-Service project does not use ECDH or any direct BouncyCastle cryptographic operations, this was identified as a false positive.

**I think I made a mistake as for some reason I changed the name of the dependency check and it still over wrote it.**

I created a suppression.xml file to suppress CVE-2015-7940 and updated my pom.xml file to include a reference to the suppression file. After rerunning the dependency check, the updated report confirmed the fix.



This demonstrates that the suppression file was successfully recognized and that the false-positive vulnerability is now hidden from the report, as recommended in DevSecOps best practices.