



snyk

SNYK REPORT SUMMARY

Giorgio Chirico

Sommario

Introduzione al report	3
Elenco delle dipendenze	4
Dipendenza spring-boot-starter-web@3.5.5	4
Dipendenza spring-boot-starter@3.5.5.....	5
Dipendenza xmlrpc-client@3.1.3 con xmlrpc-common@3.1.3	5
Dipendenza poi-ooxml@5.5.0 con commons-lang3@3.17.0	6

Indice delle figure

Figura 1 vulnerabilità per spring-boot-starter-web	4
Figura 2 vulnerabilità per spring-boot-starter	5
Figura 3 vulnerabilità per xmlrpc-client	5
Figura 4 vulnerabilità per poi-ooxml	6

Introduzione al report

Questo report è un'estratto contenente le informazioni della dashboard di Snyk. Tale piattaforma integra le informazioni da diverse knowledge base per threat intelligence, come i framework MITRE.

L'architettura fondamentale dell'applicazione è stata strutturata tenendo conto delle criticità segnalate da Snyk, di modo da ridurre se non annullare l'impatto conseguente ad un eventuale sfruttamento delle vulnerabilità note.

Per la gran parte se non tutte le seguenti vulnerabilità, Snyk non ha trovato nessun exploit pubblico associato, né un Proof-Of-Concept che ne dimostri la sfruttabilità via metodo noto. Pertanto, queste vulnerabilità sono solo una constatazione di possibili debolezze della struttura, documentate come parte di una (potenziale) superficie d'attacco da monitorare e ridurre nel tempo.

Una vulnerabilità diventa una minaccia, con impatto negativo sui processi, solo quando esiste un modo per sfruttarla. Inoltre, avere un exploit per queste vulnerabilità non implica un impatto significativo sull'operatività dell'applicazione o sulla continuità delle operazioni di business.

Elenco delle dipendenze

Le seguenti vulnerabilità sulle dipendenze sono ordinate per "priority score".

Dipendenza [spring-boot-starter-web@3.5.5](#)

[HIGH SEVERITY] Relative Path Traversal:

- Vedi [CVE-2025-55752](#) associato.
- Vedi [CWE-23](#) associato.

[HIGH SEVERITY] Incorrect Authorization:

- Vedi [CVE-2025-41249](#) associato.
- Vedi [CWE-863](#) associato.

[MEDIUM SEVERITY] Improper Resource Shutdown or Release:

- Vedi [CVE-2025-61795](#) associato.
- Vedi [CWE-404](#) associato.

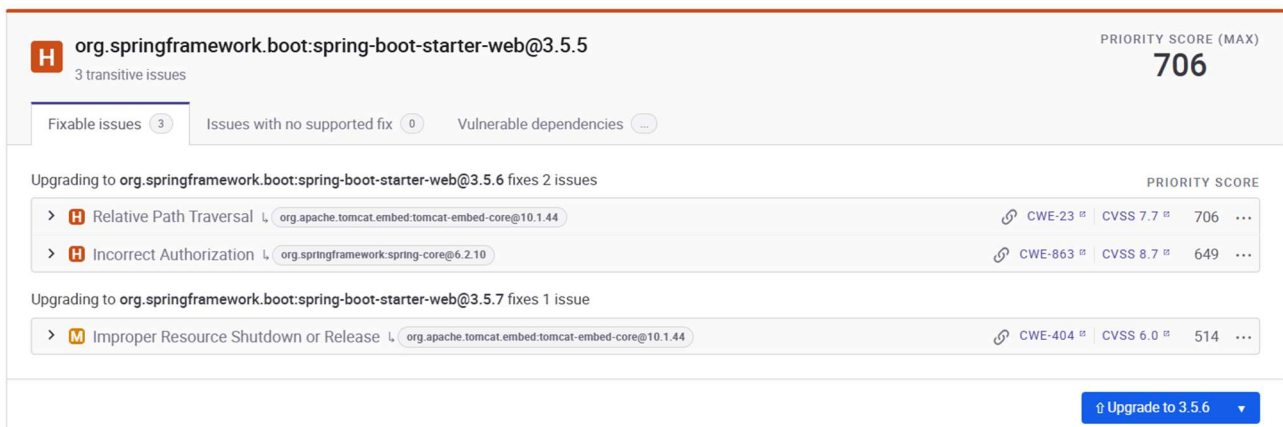


Figura 1 vulnerabilità per `spring-boot-starter-web`

Dipendenza [spring-boot-starter@3.5.5](#)

[HIGH SEVERITY] Incorrect Authorization:

- Vedi [CVE-2025-41249](#) associato.
- Vedi [CWE-863](#) associato.

[MEDIUM SEVERITY] External Initialization of Trusted Variables or Data Stores:

- Vedi [CVE-2025-11226](#) associato.
- Vedi [CWE-454](#) associato.

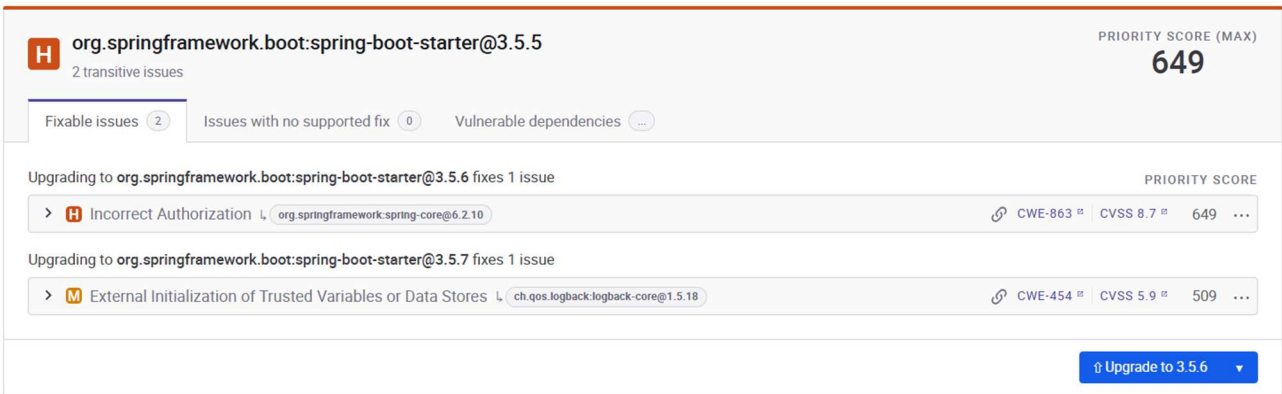


Figura 2 vulnerabilità per `spring-boot-starter`

Dipendenza [xmlrpc-client@3.1.3](#) con [xmlrpc-common@3.1.3](#)

[CRITICAL SEVERITY] Deserialization of Untrusted Data:

- Vedi [CVE-2019-17570](#) associato.
- Vedi [CVE-2016-5003](#) associato.
- Vedi [CWE-502](#) associato.




Figura 3 vulnerabilità per `xmlrpc-client`

Dipendenza poi-ooxml@5.5.0 con comons-lang3@3.17.0


[HIGH SEVERITY] Uncontrolled Recursion:

- Vedi [CVE-2025-48924](#) associato.
- Vedi [CWE-674](#) associato.

 **org.apache.poi:poi-ooxml@5.5.0**
1 transitive issue

PRIORITY SCORE (MAX)
440

Fixable issues **0** | Issues with no supported fix **1** | Vulnerable dependencies **...**

>  Uncontrolled Recursion

org.apache.commons:commons-lang3@3.17.0

[CWE-674](#) ¹² | [CVSS 8.8](#) ¹² | 440 ...

Figura 4 vulnerabilità per poi-ooxml