BOLETÍN DE ALERTA

Boletín Nro.: 2022-30
Fecha de publicación: 06/07/2022
Tema: Vulnerabilidad crítica de inyección *SpEL* en *Spring Data MongoDB*

Productos afectados:

- Spring Data MongoDB 3.4.0.
- Spring Data MongoDB 3.3.0 al 3.3.4.
- Spring Data MongoDB versiones anteriores no soportadas.

Descripción:

Se ha reportado una vulnerabilidad crítica en *Spring Data MongoDB*, que permitiría a un atacante realizar inyección *Spring Expression Language* (*SpEL*) para realizar ejecución remota de código (*RCE*).

La vulnerabilidad identificada como CVE-2022-22980 de severidad crítica y puntuación de 9.8. Esta vulnerabilidad se debe al uso de métodos de consulta *@Query* o *@Aggregation-annotated* en expresiones *SpEL,* que contienen marcadores de posición de parámetros para dicha consulta, cuyos datos de entrada no fueron correctamente validados.

Actualmente para esta vulnerabilidad, existen varios PoC publicados en internet.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar ejecución remota de código (RCE) en el sistema afectado.

Solución:

Se recomienda actualizar las versiones *Spring Data MongoDB 3.4.x* a *3.4.1+* y *3.3.x* a *3.3.5+*, siguiendo los pasos proveídos en el siguiente enlace:

- https://spring.io/guides/gs/accessing-data-mongodb/

Adicionalmente, se sugiere realizar las siguientes acciones para mitigación de las aplicaciones que no pueden actualizarse a las versiones anteriores:

- Reescribir las declaraciones de consulta o agregación para usar referencias de parámetros (“[0]” en lugar de “?0") dentro de la expresión.
- Validar los parámetros antes de llamar al método de consulta.
- Reconfigurar el repositorio de fábrica *bean* a través de *BeanPostProcessor* con el método *QueryMethodEvaluationContextProvider* .

Información adicional:

- https://portswigger.net/daily-swig/spring-data-mongodb-hit-by-another-critical-spel-injection-flaw
- https://nvd.nist.gov/vuln/detail/CVE-2022-22980
- https://spring.io/guides/gs/accessing-data-mongodb/
- https://github.com/trganda/dockerv/tree/master/vuln/spring/spring-data-mongodb/CVE-2022-22980
- https://github.com/trganda/CVE-2022-22980