USTIC-AV 03/22. Vulnerabilidades en Java Spring, una de ellas Zero Day crítica (01/04/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, **avisa** de la publicación este pasado 31 de marzo de **tres vulnerabilidades,** una de ellas de tipo zero-day**,** que afectan a **Java Spring**:

1. **Spring Core:** RCE Zero-day en Spring Core (*Spring4Shell*), con severidad **crítica** e identificador CVE-2022-22965;
2. **Spring Framework:** DoS en Spring Framework, descubierta por 4ra1n, con severidad media e identificador CVE-2022-22950;
3. **Spring Cloud Function:** RCE en Spring Cloud Function, descubierta por m09u3r, con severidad media e identificador CVE-2022-22963.

Detalle

1. Spring Core: RCE Zero-Day en Spring Core (*Spring4Shell*), con severidad crítica e identificador CVE-2022-22965.

Se ha hecho pública una **vulnerabilidad** de tipo **zero-day** que afecta al **framework Spring Core Java**, plataforma de código abierto que proporciona soporte de infraestructura integral para desarrollar aplicaciones Java, muy popular entre los desarrolladores de software.

Esta vulnerabilidad, catalogada como **crítica**, se le ha asignado el identificador CVE-2022-22965 y se le ha denominado ***Spring4Shell.*** **En determinadas circunstancias, permite que un atacante ejecute código arbitrario de forma remota (RCE)**, si bien, inicialmente se pensó que afectaría a todas las aplicaciones de Spring que se ejecutan en Java 9 o superior, se ha determinado que existen requisitos específicos que se deben cumplir para que una aplicación de Spring sea vulnerable.

De esta forma, la vulnerabilidad *Spring4Shell* afecta a las aplicaciones Spring MVC y Spring WebFlux que se ejecutan en JDK 9+. El *exploit* requiere que la aplicación se ejecute en Tomcat como un despliegue WAR. Si la aplicación se despliega como un JAR ejecutable de Spring Boot (configuración por defecto) no es vulnerable.

La explotación de esta vulnerabilidad requiere un *endpoint* con *DataBinder* habilitado y depende en gran medida del contenedor de *servlets* de la aplicación.

No obstante**, lo más preocupante ha sido la filtración de un exploit para aprovechar esta vulnerabilidad** que, aunque fue eliminado a las pocas horas, algunos investigadores pudieron descargar el código y realizar las pertinentes pruebas, confirmando que la vulnerabilidad es explotable.

Desde la plataforma REYES se están desarrollando listas negras para esta vulnerabilidad con los indicadores de compromiso proporcionados por nuestras fuentes, aunque por el momento no se ha encontrado nada relevante.

2. Spring Framework: DoS en Spring Framework, descubierta por 4ra1n, con severidad media e identificador CVE-2022-22950.

Asimismo, se ha notificado otra vulnerabilidad, catalogada con una criticidad media, por la que un usuario podría proporcionar una expresión SpEL (Spring Expression Language) especialmente diseñada para causar una condición de denegación de servicio (DoS) en Spring Framework. Se ha asignado el identificador CVE-2022-22950 para esta vulnerabilidad.

3. Spring Cloud Function: RCE en Spring Cloud Function, descubierta por m09u3r, con severidad media e identificador CVE-2022-22963.

Por último**,** se ha notificado **otra vulnerabilidad** que afecta a Spring Cloud Function, que **permite a los desarrolladores escribir funciones independientes en la nube utilizando las características de Spring**. Estas aplicaciones se pueden implementar en servidores, como por ejemplo Apache Tomcat, como paquetes independientes con todas las dependencias requeridas.

Esta vulnerabilidad, catalogada con una **criticidad media**, a la que se le asignó el CVE-2022-22963, y de la que **ya se ha publicado el parche**, **aprovecha una deserialización insegura de los argumentos utilizados en la función Spring Cloud, lo que permite que un atacante pueda ejecutar comandos de forma remota**. En ciertas configuraciones la explotación de este problema es sencilla, ya que solo requiere que un atacante envíe una solicitud POST diseñada a un sistema vulnerable. No obstante, la explotación en otras configuraciones requerirá que el atacante realice una investigación adicional para encontrar solicitudes que sean efectivas.

Debido a la criticidad, sobre todo de *Spring4shell*, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a la vulnerabilidad.

Recursos Afectados

- **Spring Core (Spring4Shell):**

  Se necesitan requisitos específicos para estar directamente afectados por ***Spring4Shell*** (CVE-2022-22965):

  - JDK, versión 9 o superior;
  - Apache Tomcat como el contenedor Servlet;
  - empaquetado como WAR;
  - dependencias *spring-webmvc* o *spring-webflux*;
  - Spring Framework, versiones:
    - desde 5.3.0 hasta 5.3.17;
    - desde 5.2.0 hasta 5.2.19;
    - y versiones anteriores.

  Para consultar la lista de fabricantes afectados, consulte la página de información de CERT/CC.

- **Spring Framework, versiones:**
  - desde 5.3.0 hasta 5.3.16;
  - las versiones más antiguas y sin soporte también se ven afectadas.
- **Spring Cloud Function, versiones:**
  - 3.1.6;
  - 3.2.2;
  - las versiones más antiguas y sin soporte también se ven afectadas.

Recomendaciones Actualizadas (04/04/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos:

Mitigación

1º. Solución a las vulnerabilidades:

- **Spring Core (Spring4Shell):**

  En las últimas horas se ha hecho público un parche que aborda la vulnerabilidad CVE-2022-22965 y que puede ser localizado en el siguiente enlace:

  - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

  Adicionalmente, el blog de Praetorian describe una forma de mitigar parcialmente los ataques a la vulnerabilidad *Sprin g4Shell* (CVE-2022-22965) al no permitir que se pasen patrones específicos a la funcionalidad *Spring Core DataBinder*.

- **Spring Framework:**

  Actualizar a la versión 5.3.17 o superiores.

- **Spring Cloud Function:**

  Actualizar a las versiones 3.1.7 o 3.2.3.

Por el momento, se desconocen medidas de mitigación alternativas a las ya mencionadas para solucionar estas vulnerabilidades. **Os seguiremos informando.**

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Spring4shell]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por su atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud