| Nro. Alerta: | EC-2022-57 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 05-abril-2022 | **Vulnerabilidades en Spring Framework** | Versión 1.0 |

## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad
**Tipo de incidente:** Sistema y/o Software Abierto
**Nivel de riesgo:** Alto

## II. ALERTA

En el transcurso de la última semana de marzo del 2022 se han dado a conocer diferentes vulnerabilidades asociadas a Spring framework.

**Figura 1.** Ilustración relacionada a Spring
**Fuente:** SPRING

## III. INTRODUCCIÓN

Spring es un framework Open Source que permite la creación de aplicaciones de todo tipo en Java, Kotlin y Groovy; este framework de código abierto. Según estudios de diferentes fuentes; se estima que entre alrededor del 70% al 80% de las aplicaciones WEB son desarrolladas con este Framework.

A finales de marzo de 2022, se dieron a conocer vulnerabilidades que afectan al framework de Spring; las mismas que, permitirían tomar remotamente el control de aplicaciones vulnerables. A continuación, se listan las vulnerabilidades asociadas:



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| Nro. Alerta: | EC-2022-57 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 05-abril-2022 | **Vulnerabilidades en Spring Framework** | Versión 1.0 |

| ÍTEM | CVE | DESCRIPCIÓN |
|---|---|---|
| **1** | CVE-2022-22965 | Esta vulnerabilidad conocida como Spring4Shell pasa por alto el parche para CVE-2010-1622, lo que hace que CVE-2010-1622 vuelva a ser explotable. Se considera que esta vulnerabilidad tiene un mayor impacto, ya que afecta a la biblioteca principal y, por lo tanto, todos los proyectos de Spring se ven potencialmente afectados. |
| **2** | CVE-2022-22963. | En las versiones 3.1.6, 3.2.2 y anteriores de Spring Cloud Function, cuando se utiliza la funcionalidad de enrutamiento, es posible que un usuario proporcione un SpEL[1] especialmente diseñado como una expresión de enrutamiento que puede resultar en la ejecución remota de código y el acceso a los recursos locales. |

**Tabla 1.** Vulnerabilidades en Spring Framework
**Fuente:** GENBETA

## IV. **VECTOR DE ATAQUE:** RCE

A continuación, se describe el vector de ataque de estas vulnerabilidades.

| ÍTEM | CVE | DESCRIPCIÓN |
|---|---|---|
| **1** | CVE-2022-22965 | La omisión del parche puede ocurrir porque las versiones 9 y posteriores del Kit de desarrollo de Java (JDK) brindan dos métodos de restricción de espacio aislado, lo que proporciona una ruta para explotar CVE-2010-1622 (las versiones de JDK anteriores a la 9 solo brindan un método de restricción de espacio aislado).<br><br>Según el fabricante, el vector es: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:X/RC:X |
| **2** | CVE-2022-22963. | El ataque puede ser realizado a través de la red y la explotación no requiere ninguna forma de autentificación. A continuación, se indica el vector conforme al fabricante.<br><br>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:X/RC:X |

**Tabla 2.** Vector de Ataque en referencia a vulnerabilidades en Spring Framework
**Fuente:** CISA

[1] Spring Expression Language es utilizado en toda la cartera de Spring, que admite consultas y manipulación de un gráfico de objetos en tiempo de ejecución



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| Nro. Alerta: | EC-2022-57 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS<br>**ALERTA DE SEGURIDAD** | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 05-abril-2022 | **Vulnerabilidades en Spring Framework** | Versión 1.0 |

## V. IMPACTO:

A continuación, se mencionan el impacto de estas vulnerabilidades:

| ÍTEM | CVE | DESCRIPCIÓN |
|---|---|---|
| **1** | CVE-2022-22965 | Esta vulnerabilidad crítica permitiría a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a una inapropiada validación de inputs. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total de un sistema vulnerable. |
| **2** | CVE-2022-22963. | Spring Cloud Functions pueden ser utilizadas en funciones tipo serverless desplegadas en los múltiples proveedores Cloud. Una explotación exitosa podría permitir comprometer las cuentas u otros servicios publicados en la nube. |

**Tabla 3.** Impacto en referencia a vulnerabilidades en Spring Framework
**Fuente:** TARLOGIC

## VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Actualizar las versiones afectadas de Spring Framework; en este sentido, si utiliza versiones 5.3.x deben actualizar a 5.3.18+; mientras que para las versiones 5.2.x deben actualizar a 5.2.20+.
- Actualizar Spring Cloud Function a las versiones: 3.1.7 y 3.2.3, según corresponda.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

## VII. REFERENCIAS:

Akamai. (31 de 03 de 2022). *Akamai*. Obtenido de Akamai: https://www.akamai.com/blog/security/spring-core-spring4shell-zero-day/_jcr_content

CERT. (04 de 04 de 2022). *CERT Carnegie Mellon University*. Obtenido de CERT Carnegie Mellon University: https://kb.cert.org/vuls/id/970766

Merino, M. (1 de 04 de 2022). *Genbeta*. Obtenido de Genbeta: https://www.genbeta.com/desarrollo/log4shell-fue-grave-algunos-expertos-creen-que-nueva-vulnerabilidad-spring4shell-podria-ser-peor

Pahino, R. (s.f.). *Campus MVP*. Obtenido de Campus MVP: https://www.campusmvp.es/recursos/post/que-son-spring-framework-y-spring-boot-tu-primer-programa-java-con-este-framework.aspx#:~:text=Si%20desarrollas%20con%20Java%2C%20o,en%20Java%2C%20Kotlin%20y%20Groovy.

Spring. (s.f.). *Spring*. Obtenido de Spring: https://spring.io/

TANZU, V. (31 de 03 de 2022). *VMWARE TANZU*. Obtenido de VMWARE TANZU: https://tanzu.vmware.com/security/cve-2022-22965

TANZU, V. (31 de 03 de 2022). *VMWARE TANZU*. Obtenido de VMWARE TANZU: https://tanzu.vmware.com/security/cve-2022-22965

VulDB. (02 de 04 de 2022). *VulDB*. Obtenido de VulDB: https://vuldb.com/es/?id.196076