USTIC-AV 16/22. Vulnerabilidad crítica en Apache Commons Text (20/10/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, del Centro Criptológico Nacional, **avisa** de la **publicación** de una **vulnerabilidad crítica** que afecta a la librería **Apache Commons Text** y que **permite a un atacante remoto** la posibilidad de **ejecutar código arbitrario (RCE).**

Detalle

Apache Commons Text es una popular biblioteca Java de código abierto con un sistema de interpolación que permite a los desarrolladores modificar, decodificar, generar y escapar cadenas en función de las búsquedas de cadenas ingresadas.

El fallo detectado, el cual ha sido catalogado bajo el CVE-2022-42889, **es una vulnerabilidad crítica (*puntuación CVSSv3 9.8*)**, **denominada "*Text4Shell*"**, causada por una evaluación de secuencias de comandos insegura por parte del sistema de interpolación que **podría desencadenar la ejecución de código arbitrario al procesar entradas maliciosas en la configuración predeterminada de la biblioteca.**

En este momento, no hay información sobre si está siendo explotada activamente, pero, debido a su gravedad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas.

Recursos Afectados

El problema afecta a las siguientes versiones:

- **Apache Commons Text** desde la **versión 1.5 hasta** la **9**, ambas incluidas.

Recomendaciones Actualizadas (20/10/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

- **Actualizar** *a la versión* ***1.10.0 de Apache Commons Text****, disponible en el siguiente enlace:*
    - *Apache Commons Text 1.10.0.*

Referencias

- CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due to insecure interpolation defaults
- GHSL-2022-018: Arbitrary Code Execution in Apache Commons Text - CVE-2022-42889
- CVE-2022-42889: Keep Calm and Stop Saying "4Shell"
- CVE-2022-42889 Detail
- Critical-Severity Flaw in Apache Commons Text Library Fixed.
- https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/12084-ccn-cert-av-17-22-vulnerabilidad-en-apache-commons-text.html

---

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Text4Shell1022]*

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

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud