Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Servicio aduanero confirma fallas en sistemas informáticos, pero garantiza operaciones de embarque y desembarque

19/Octubre/2022

Contenido

INTRODUCCIÓN

Una falla de ejecución remota de código en la biblioteca Apache Commons Text de código abierto tiene a algunas personas preocupadas de que pueda convertirse en el próximo Log4Shell. Sin embargo, la mayoría de los investigadores de ciberseguridad dicen que no es tan preocupante.

VULNERABILIDAD CVE-2022-42889 EN APACHE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_10_19_02
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/19/2022
Es día cero (0 day):	No

RESUMEN

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.

Por ejemplo, pasar la búsqueda de cadenas `${base64Decoder:SGVsbG9Xb3JsZCE=}` al sistema de interpolación haría que la biblioteca la convirtiera a su valor decodificado en base64 de 'HelloWorld!'.

La nueva vulnerabilidad CVE-2022-42889 en Apache Commons Text, denominada "Text4Shell", es causada por una evaluación de secuencias de comandos insegura por parte del sistema de interpolación que podría desencadenar la ejecución de código al procesar entradas maliciosas en la configuración predeterminada de la biblioteca.

"Comenzando con la versión 1.5 y continuando hasta la 1.9, el conjunto de instancias de búsqueda predeterminadas incluía interpoladores que podrían resultar en la ejecución de código arbitrario o contacto con servidores remotos", detalla un desarrollador en la lista de correo de Apache.

"Las aplicaciones que usan los valores predeterminados de interpolación en las versiones afectadas pueden ser vulnerables a RCE o al contacto no intencional con servidores remotos si se usan valores de configuración que no son de confianza".

"Se recomienda a los usuarios que actualicen a Apache Commons Text 1.10.0, que desactiva los interpoladores problemáticos de forma predeterminada".

El problema fue descubierto por el analista de amenazas de GitHub, Álvaro Muñoz , y se informó a Apache el 9 de marzo de 2022.

Sin embargo, los desarrolladores de la biblioteca de código abierto tardaron 7 meses, hasta el 12 de octubre de 2022, en publicar una corrección en la versión 1.10.0, que deshabilita la interpolación.

¿Deberías preocuparte?

Debido al despliegue generalizado de la biblioteca vulnerable, y dado que la falla afecta a las versiones que datan de 2018, inicialmente a algunos les preocupaba que pudiera causar un daño generalizado, como vimos con la vulnerabilidad Log4Shell .

Sin embargo, un informe de Rapid7 rápidamente puso freno a estas preocupaciones, explicando que no todas las versiones entre la 1.5 y la 1.9 parecen vulnerables y que su potencial de explotación estaba relacionado con la versión de JDK utilizada.

Incluso con un exploit de prueba de concepto (PoC) actualizado que usa el motor JEXL como una ruta de exploit que evita la limitación de JDK, los investigadores aún no están muy preocupados.

```
[INFO] --- exec-maven-plugin:3.1.0:java (default-cli) @ ScriptInjection ---
Available engines:
  - JEXL
Payload: ${java:version} ${script:JEXL:''.getClass().forName('java.lang.Runtime').getRuntime().exec('touch /tmp/pwned')}
Java version 19 Process[pid=44196, exitValue=0]
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
```

Nuevo PoC trabajando en todas las versiones vulnerables

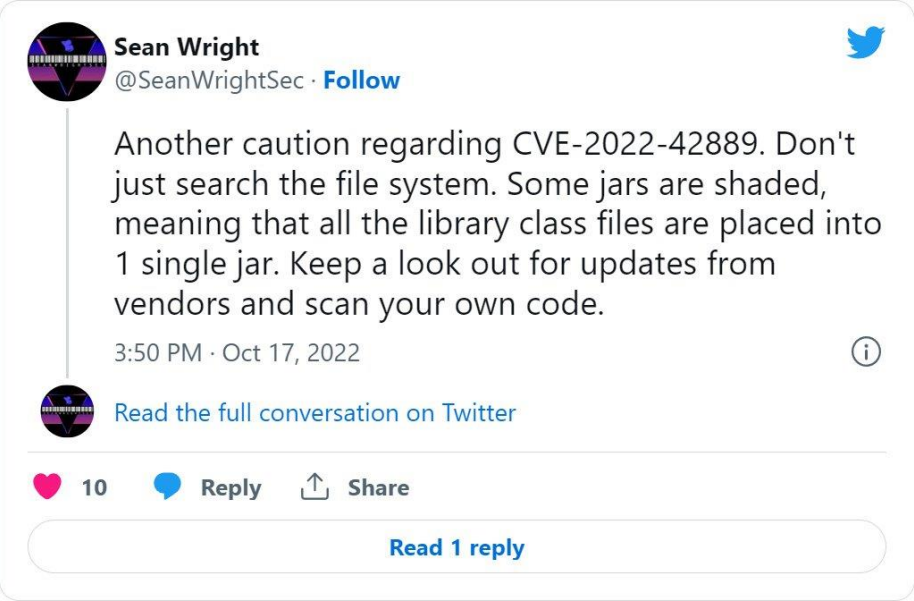
Además, el equipo de seguridad de Apache ha dicho que el alcance de la falla no es tan grave como Log4Shell, explicando que la interpolación de cadenas es una característica documentada. Por lo tanto, es menos probable que las aplicaciones que usan la biblioteca pasen inadvertidamente entradas no seguras sin validación.

Si bien la falla de gravedad crítica permaneció sin parchear durante siete meses y estuvo expuesta a intentos de explotación, no ha habido informes de abuso en la naturaleza incluso después de que se lanzaron las vulnerabilidades.

Si bien es probable que veamos a algunos actores de amenazas explotar CVE-2022-42889 en el futuro, probablemente tendrá un alcance limitado.

Por ahora, se recomienda a todos los desarrolladores que utilicen la biblioteca Apache Commons Text que actualicen a la versión 1.10 o posterior lo antes posible para corregir la falla.

El investigador de seguridad Sean Wright advierte que algunos proyectos de Java mantienen todos los archivos de clase de biblioteca en un solo contenedor y deberán escanearse de forma independiente.



Para ayudar a encontrar versiones vulnerables de la biblioteca Apache Commons Text, Silent Signal ha lanzado un complemento Burp que puede escanear aplicaciones en busca de componentes sin parches contra CVE-2022-42889.

Recomendaciones

- Agendar ventana de mantenimiento para aplicar la actualización de Apache.

- Se recomienda escanear con el complemento Burp para detectar vulnerabilidades accesibles mediante CVE-2022-42889.

- Mantener respaldo de sus servidores previo a la actualización, para mitigar cualquier contingencia.

Noticia Completa

https://devel.group/blog/vulnerabilidad-en-apache-commons-text/

Información sobre la actualización recomendada

https://lists.apache.org/thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente