Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

APACHE SOLUCIONA VULNERABILIDAD CRÍTICA EN STRUTS 2

12/ 12 / 2023

CONTENIDO

INTRODUCCIÓN

La Apache Software Foundation ha abordado proactivamente una vulnerabilidad crítica de ejecución remota de código (RCE) en Apache Struts 2, un popular marco de desarrollo de código abierto. La vulnerabilidad, conocida como CVE-2023-50164, estaba vinculada a una falla en la lógica de carga de archivos que permitía el cruce de rutas no autorizadas. En ciertos escenarios, esto facilitaba la carga de archivos maliciosos, posibilitando la ejecución de código arbitrario.

APACHE SOLUCIONA VULNERABILIDAD CRÍTICA EN STRUTS 2

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

ID de alerta:	DSOC-CERT_2023_12_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/12/2023
Es día cero (0 day):	No

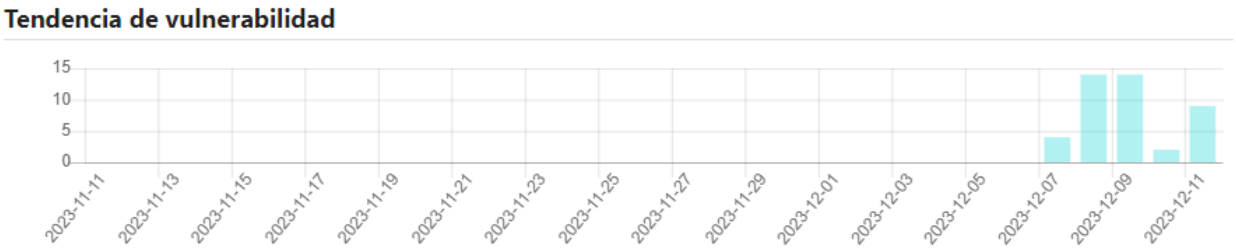
RESUMEN

La Apache Software Foundation ha respondido de manera proactiva a una vulnerabilidad crítica de ejecución remota de código (RCE) en el popular marco de desarrollo de código abierto, Apache Struts 2. La vulnerabilidad, identificada como CVE-2023-50164, estaba relacionada con una deficiencia en la lógica de carga de archivos que permitía el cruce de rutas no autorizadas y, en ciertas circunstancias, posibilitaba la carga de archivos maliciosos para lograr la ejecución de código arbitrario.

La explotación exitosa de esta vulnerabilidad podría haber permitido a un atacante remoto manipular los parámetros de carga de archivos, habilitando el recorrido de rutas que, en última instancia, podría conducir a la ejecución remota de código en sistemas afectados.

Según el aviso publicado por la Apache Software Foundation, “Un atacante puede manipular los parámetros de carga de archivos para habilitar el recorrido de rutas y, en algunas circunstancias, esto puede llevar a cargar un archivo malicioso que se puede usar para realizar la ejecución remota de código”.

La fundación insta a todas las organizaciones que utilizan Apache Struts 2 a actualizar a las versiones 2.5.33 o Struts 6.3.0.2 o superiores para mitigar esta vulnerabilidad crítica.



La vulnerabilidad afecta a las siguientes versiones de Apache Struts:

Struts 2.3.37 (EOL)

Struts 2.5.0 – Struts 2.5.32

Struts 6.0.0 – Struts 6.3.0

Aunque no hay evidencia de que la vulnerabilidad haya sido explotada activamente en ataques del mundo real, es crucial recordar que vulnerabilidades anteriores en Apache Struts han sido aprovechadas por actores de amenazas para perpetrar ataques significativos, como el caso CVE-2017-5638, que se utilizó en el ataque a la agencia de informes crediticios Equifax en 2017.

La revelación de la vulnerabilidad CVE-2023-50164 por parte de investigadores de seguridad ha proporcionado detalles técnicos y una prueba de concepto (POC) que plantean una situación inquietante. El proceso de explotación se inicia al priorizar la carga de archivos, permitiendo a los atacantes manipular el parámetro uploadFileName para establecer una ruta, lo que finalmente resulta en la carga de un archivo shell.jsp en el servidor de la víctima.

```
POST /s2_066_war_exploded/upload.action HTTP/1.1
Host: localhost:8080
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5WJ61X4PRwyYKlip
Content-Length: 593

------WebKitFormBoundary5WJ61X4PRwyYKlip
Content-Disposition: form-data; name="upload"; filename="poc.txt"
Content-Type: text/plain

test


------WebKitFormBoundary5WJ61X4PRwyYKlip
Content-Disposition: form-data; name="caption";


{{randstr(4097,4097)}}

------WebKitFormBoundary5WJ61X4PRwyYKlip--
```

Dada la naturaleza crítica de la vulnerabilidad y la posible ejecución remota de código asociada, se insta a la comunidad de desarrolladores y a las organizaciones a actuar de manera inmediata para parchear sus sistemas Apache Struts 2. Mantenerse actualizado con las últimas versiones y parches es esencial para garantizar la seguridad de las aplicaciones web y protegerse contra posibles amenazas cibernéticas.

RECOMENDACIONES

- Se recomienda que mantenga actualizado su software, como el sistema operativo y las aplicaciones que utiliza. Esto le ayudará a asegurarse de que esté utilizando las versiones más recientes, lo que suele incluir correcciones de seguridad importantes.

NOTICIA COMPLETA

https://devel.group/blog/apache-soluciona-vulnerabilidad-critica-en-struts-2/

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