Informe de Amenazas
CCN-CERT IA-22/17

MEDIDAS DE SEGURIDAD
Vulnerabilidad de Struts

(CVE-2017-9805)

Septiembre 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.09.08 09:14:30 +02'00'

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, del **Sector Público** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. INTRODUCCIÓN

Struts es una herramienta de soporte para el desarrollo de aplicaciones Web que sigue el patrón MVC (Modelo Vista Controlador) bajo la plataforma Java EE (*Java Enterprise Edition*), que se instala sobre un servidor Apache. Struts se desarrollaba como parte del proyecto Jakarta de la Apache Software Foundation, pero actualmente es un proyecto conocido como Apache Struts.

El 29 de enero de 2017, se hizo pública una vulnerabilidad con código CVE-2017-5638, que permitiría a un atacante ejecutar órdenes remotas sobre un servidor a través de un contenido subido al componente de análisis Jakarta Multipart, el cual es utilizado por algunas aplicaciones de Struts. Esta vulnerabilidad afecta a las siguientes versiones de Struts:

- Versiones 2.3.x anteriores a 2.3.32
- Versiones 2.5.x anteriores a 2.5.10.1

Para dicha vulnerabilidad se elaboró el informe CCN-CERT IA-09/17, en el que se recogía el procedimiento a seguir para solucionar el problema.

El 16 de agosto de 2017 se hizo pública una nueva vulnerabilidad (CVE-2017-9805) que afecta a este software, que de la misma forma que la anterior vulnerabilidad, **permitiría a un atacante ejecutar órdenes remotas** sobre un servidor con las siguientes versiones de Struts:

- **Versiones 2.3.x anteriores a 2.3.34**
- **Versiones 2.5.x anteriores a 2.5.13**

El error de la aplicación [Ref. 1] reside en el manejo del plugin Rest de Struts al usar XStreamHandler al deserializar un XML enviado a la aplicación de forma remota.

3. MEDIDAS PALIATIVAS

Para solucionar la vulnerabilidad basta con **actualizar Apache Struts** a la **versión 2.3.34 ó 2.5.13**. Como primera medida, de manera más inmediata, se puede realizar lo siguiente:

- Eliminar el plugin REST de Struts si no se está utilizando.
- Si se está utilizando el plugin REST, limitarlo a tratar únicamente contenido HTML y JSON mediante la inclusión de la siguiente directiva:

```
<constant name=”struts.action.extension” value=”xhtml,,json” />
```

Se recomienda consultar la web del fabricante [Ref. 1] para obtener más detalles sobre esta vulnerabilidad.

4. DETECCIÓN

Si su sistema ha sido víctima de un ataque utilizando esta vulnerabilidad, puede realizar las siguientes acciones para intentar identificar las acciones realizadas por el atacante:

1. Revisar el uso del usuario root del sistema en los días del ataque.
2. Revisar la lista de usuarios, para verificar que no se hayan creado nuevos.
3. Revisar la configuración de iptables en el servidor. El atacante podría haber intentado deshabilitarlo.
4. Revisar los accesos del usuario que ejecuta la página web con Struts. Revisar si se han creado ficheros, carpetas, o procesos con dicho usuario.
5. Revisar si se han creado procesos o servicios fuera del uso normal.
6. Revisar las conexiones salientes desde los equipos atacados, conexiones SSH, conexión por FTP/SFTP, conexiones a servicios de almacenamiento en la nube como Dropbox, Google Drive…
7. Revisar si se han creado tareas en el cron del sistema para verificar la no instalación de tareas programadas.
8. Revisar la creación y modificación de ficheros en los días que ha durado el ataque, para ello se puede utilizar el siguiente comando:

```
find / -type f -mtime -<número de días>
```

   Por ejemplo, para realizar la búsqueda durante los últimos 3 días:

```
find / -type f -mtime -3
```

9. Revisar si se han creado páginas web en el servidor fuera del uso normal del servidor, por si se han generado webshells.

5. RECOMENDACIONES

Para prevenir futuros ataques de este tipo se recomienda realizar las siguientes acciones:

- Mantener todos los sistemas **actualizados**. Para ello es conveniente disponer de una política de parches de seguridad que permita la actualización de los sistemas en el menor tiempo posible.
- Disponer de un **sistema de copias de seguridad** adecuado que almacene copias de seguridad de los sistemas de manera periódica, ya que nos permitiría restaurar los servicios en el caso de que fueran objeto de una denegación de servicio.
- **Limitar los privilegios del usuario** que ejecuta la página web con Apache Struts, permitiendo únicamente el acceso a los ficheros que se ubiquen dentro del

espacio web de trabajo, de este modo se impide que en caso de intrusión se pueda tener acceso a recursos externos (unidades montadas, espacio del usuario, etc.)

- Aplicar las medidas de seguridad indicadas en las diferentes **guías CCN-STIC** para mantener un nivel de seguridad de los sistemas lo más alto posible.

6. REFERENCIAS

[Ref. 1] Información sobre la vulnerabilidad CVE-2017-9805

https://cwiki.apache.org/confluence/display/WW/S2-052