CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

ASS-AATIC-122-2022
30 de junio de 2022

Máster
Idannia Mata Serrano, Subgerente a.i,

Máster
Vanessa Carvajal Carmona, jefe
Subárea Seguridad de Tecnologías de Información
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150

Estimadas señoras:

ASUNTO:	**Oficio asesoría referente a las acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta "Log4J".**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno específicamente en su rol de asesor, esta Auditoría informa sobre la importancia de implementar acciones anticipadas, a fin de evitar la materialización de riesgos en materia de Ciberseguridad, generados por la herramienta "Log4J" una vez que se normalicen las operaciones en la Institución y entre en funcionamiento la plataforma tecnológica de la Caja.

Al respecto, Log4J es una utilidad de registro de código abierto desarrollado en el lenguaje Java, el cual es ampliamente utilizada por aplicaciones y servicios en la nube. En ese sentido, el aprovechamiento de la solución habitualmente se da en múltiples sistemas operativos e inclusive equipamiento (hardware) que incluye componentes de software basados en esa tecnología.

Lastimosamente, los hackers identificaron una vulnerabilidad en esa herramienta y han puesto en riesgo a una importante cantidad de organizaciones, por ello los expertos han catalogado esta amenaza como crítica (la debilidad fue valorada con un 10, máxima criticidad otorgable), según cita el proveedor tecnológico "Trend Micro"[1] en la nota "¿En qué consiste la vulnerabilidad de Apache Log4J (Log4Shell)[2]?":

> *"2021 fue un año muy intenso para las vulnerabilidades de día cero que tuvieron su coronación con Log4Shell, el cual es un fallo crítico encontrado en la ampliamente utilizada biblioteca de inicio de sesión con base en Java, Apache Log4j. Oficialmente identificada como CVE-2021-44228, el Common Vulnerability Scoring System (CVSS) le otorga una puntuación de gravedad de 10 en una escala de 10 (CVSS v3.1)."*

Además, en ese mismo artículo se menciona la advertencia que emitieron los entes especializados a nivel internacional, debido al impacto y la probabilidad de materializarse un riesgo cibernético, citando:

> *"Las posteriores noticias de ataques observados de libre circulación provocaron que diversas agencias de ciberseguridad nacional emitieran alertas, incluida la Agencia de seguridad cibernética e infraestructura (CISA) de EE. UU., el Centro nacional de ciberseguridad (NCSC) del Reino Unido y el Centro canadiense de ciberseguridad. Debido a la popularidad de Apache Log4j, cientos de millones de dispositivos podrían verse afectados."*

En resumen, las fuentes indican que el funcionamiento de los ataques consiste en perpetrar la librería Log4J y realizar ejecuciones remotas (desde cualquier parte del mundo) y así obtener información valiosa de la red organizacional. En otras palabras, la vulnerabilidad ha sido aprovechada por los hackers para el robo de información, penetración de sistemas, denegar servicios e implantar Ransomware, para solicitar a cambio una recompensa.

[1] Trend Micro es uno de los mayores proveedores de seguridad de Internet y antivirus en el mundo con más de 250 millones usuarios.
[2] Enlace a nota: https://www.trendmicro.com/es_es/what-is/apache-log4j-vulnerability.html

Lo anterior, por medio de páginas web, aplicaciones de escritorio, sistemas operativos de distintos dispositivos (servidores, unidades de cómputo, tabletas, celulares, equipo de telecomunicaciones), firmware, entre otros medios.

Un ejemplo de los países públicamente afectados por la vulnerabilidad supracitada fue en Bélgica, según detalla el espacio informativo español denominado: "Escudo Digital" en la publicación del 22 de diciembre del 2021, titulada "El Ministerio de Defensa de Bélgica, atacado por Log4Shell":

> *"La vulnerabilidad Log4Shell se ha convertido en la peor pesadilla prenavideña para las plataformas de Internet y los CISOS de todo el mundo. Los ataques se repiten miles de veces y, a la fuerza, terminan por acertar. Según informa la web Xacata, el Ministerio de Defensa de Bélgica ha sido el primer país de la OTAN que ha reconocido públicamente haber sido víctima de este problema.*
>
> *Xacata remite a The Register, que informa que el organismo de seguridad belga detectó el pasado jueves un ciberataque a su red informática con acceso a Internet. Decidieron "tomar medidas de cuarentena para aislar las partes afectadas" con el fin de mantener operativa la red de defensa del país europeo. Sin embargo, "algunas actividades del ministerio se vieron paralizadas durante varios días".*
>
> *El portavoz belga del Ministerio de Defensa, Olivier Severin reconoció que los atacantes habían utilizado la vulnerabilidad Log4Shell. No dio muchos más detalles, ni el tipo de afectación del sistema. Se ignoran de momento las secciones afectadas, pero está claro que ha afectado incluso al servicio de respuestas vía Facebook del Ministerio. Esto es lo que reza en el mensaje que acompaña a estas líneas, escrito en flamenco y en francés en la red social.*
>
> *"Debido a problemas técnicos, no podemos procesar sus solicitudes a través de www.mil.be o responder sus preguntas a través de Facebook. Estamos trabajando en una solución y le agradecemos su comprensión".*
>
> *Log4Shell ha sido definida como la vulnerabilidad más crítica del año. Y es que utiliza una librería de registro Java usada por sistemas de todo el mundo. Aunque los parches se pongan a velocidad de vértigo, los problemas no paran de crecer para diversas organizaciones y están poniendo a prueba y en serios problemas a importantes multinacionales y al sistema tecnológico universal."*

Es decir, la cobertura de los hackers es toda la plataforma tecnológica que respalda los procesos organizacionales y que no han sido actualizados, tal y como lo refiere la publicación del diario nacional "La República" en la nota periodística "Vulnerabilidad crítica en los servidores Web (Log4J): Acción inmediata requerida", a saber:

> *"(…) se espera que la situación no se remedie en el futuro inmediato, dado el gran número de sistemas y dispositivos que se han visto afectados. Uno de los principales problemas que se presenta con esta corrección es el hecho de que no hay una receta estándar para arreglar la vulnerabilidad, es decir, esta será diferente según el proveedor del sistema y el código de software que utilice. Por otra parte, técnicamente, cualquier sistema basado en Apache Web Server, que comprende un tercio de los servidores expuestos a Internet alrededor del mundo según sitios especializados como https://w3techs.com/technologies/overview/web_server o https://www.wappalyzer.com/technologies/web-servers . Esto implica que uno de cada tres servidores con contenido disponible en Internet, puede ser víctima de un ataque basado en la explotación de esta vulnerabilidad."*

Para tales efectos, las siguientes recomendaciones son para contrarrestar el nivel de exposición a la vulnerabilidad de marras:

1. Mantener los sistemas operativos actualizados y aplicaciones al día, es decir, con sus respectivos parches y actualizaciones.
2. Instalar los parches específicos para solucionar la vulnerabilidad Log4j.

3. Estar pendientes de futuras actualizaciones y/o alertas que les brinden la protección o información necesaria para esta y otras amenazas.
4. Instalar soluciones de seguridad en servidores; en muchos casos, esto permitirá detectar el lanzamiento de código malicioso y detener el desarrollo del ataque.
5. Brindar mantenimiento mínimo de la plataforma tecnológica que respalda el funcionamiento de las organizaciones.
6. Es imperativo también, analizar los proveedores externos de sistemas, tanto en la nube, como internamente o alojados en servidores del proveedor para asegurarse de que se hayan tomado las medidas adecuadas para reparar o remediar las soluciones que ofrecen.

Así las cosas, el detalle de la vulnerabilidad puede ser encontrado en el sitio web https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

Bajo ese contexto, la sensibilidad del asunto demanda la atención de la CCSS a nivel del ente rector en tecnologías, en alineamiento a lo indicado en las *Normas técnicas para la gestión y el control de las Tecnologías de Información* del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la "*Seguridad y Ciberseguridad*", citando:

> *"**XI. SEGURIDAD Y CIBERSEGURIDAD***
>
> *La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*
>
> *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.*
>
> *La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*
>
> *La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.*
>
> *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."*

Por todo lo anterior, esta Auditoría da a conocer las observaciones señaladas en el presente oficio, con el fin de ser valoradas en el cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional, así como reforzar los mecanismos de ciberseguridad, de forma tal que se reduzca la posibilidad de materializarse este tipo de riesgos y eventualmente evitar incidentes como los acontecidos el pasado 31 de mayo en la CCSS ante vulnerabilidades de índole tecnológica.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.01 15:00:06 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/ghc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General -1100.
Auditoría