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

AS-AATIC-182-2022
15 de septiembre de 2022

Ingeniero
Esteban Zúñiga Chacón, jefe
Centro de Gestión Informática
GERENCIA MÉDICA-2901

Ingeniera
Guiselle Tenorio Chacón, jefe
Centro de Gestión Informática
GERENCIA ADMINISTRATIVA-1104

Ingeniero
Alexánder Solís Abarca, jefe
Centro de Gestión Informática
GERENCIA FINANCIERA-1103

Ingeniero
Giovanni Campos Alvarado, jefe
Centro de Gestión Informática
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS-1107

Ingeniero
Roy Ovares Valerio, jefe
Centro de Gestión Informática
GERENCIA LOGÍSTICA-1106

Ingeniero
Marco Vinicio González Jiménez, jefe
Centro de Gestión Informática
GERENCIA DE PENSIONES-9108

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

Estimados(as) señores (as):

ASUNTO:	**Oficio de Asesoría Referente a Nuevas Vulnerabilidades Explotadas Activamente que han sido incorporadas al Catálogo de Vulnerabilidades Conocidas.**

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 en materia de ciberseguridad sobre las nuevas vulnerabilidades que fueron incorporadas al Catálogo de Vulnerabilidades Explotadas Conocidas (KEV), las cuales afectan el manejo y resguardo de los datos, además de presentarse un alto riesgo de ingreso a las computadoras y sistemas sin el debido permiso de acceso.

ANTECEDENTES

Como es del conocimiento, el 31 de mayo 2022, se registró en horas de la madrugada un ciberataque en contra de los servidores e infraestructura de telecomunicaciones de la CCSS, el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

De esa forma, el diario La República publicó el 31 de mayo 2022, "Hackers tenían como objetivo el robo de información y las bases de datos de la Caja", detallando:

> *"Robar las bases de datos, así como otra información de la Caja y de los asegurados eran los objetivos de los hackers, según confirmó hoy el Ministerio de Ciencia y Tecnología, que ha trabajado con esta institución afectada por el ataque.*
>
> *La violación de los sistemas informáticos, que se realizó en horas de la madrugada, fue considerada como "especialmente violenta y devastadora", tanto en los servidores físicos, como en la nube.*
>
> ***La modalidad de vulneración de los sistemas informáticos utilizado por los delincuentes fue por medio de "ransomware**", el cual, consiste en el robo de información y bases de datos, sin que se conozca el responsable del daño". (La negrita no es del original)*

ASPECTOS GENERALES SOBRE EL CONCEPTO DE VULNERABILIDAD

Es importante recordar que la vulnerabilidad en términos de informática es una debilidad o fallo en un sistema que pone en riesgo la seguridad de la información, permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta. Mientras que una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información, es decir, que podría tener un potencial efecto negativo sobre algún elemento de los sistemas.

Por ende, son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas por lo que, si existe una de ellas, siempre habrá alguien que intentará explotarla, es decir, sacar provecho de su existencia.

En esta misma línea, mencionar el concepto de "riesgo", representa la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños, y se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza. Podemos mencionar como ejemplo: un hacker, un ataque de denegación de servicios, un virus, entre otros.

Figura 1
Producto de factores que representan el riesgo

Se debe mencionar que existen dos tipos: el primer tipo es conocido como teórica, mientras que el segundo tipo, y el que interesa al usuario, es el conocido como real, más conocido por todos como “Exploit”.

Estos “exploits” son las que se encuentran en las aplicaciones y sistemas operativos que se corrigen mediante parches o “hotfixs”. Muchas veces también sucede que se espera al cambio de versión para solucionar este tipo de problemas, aumentando de este modo el riesgo de ataque. En los grandes sistemas, es posible que la solución sea la corrección mediante el cambio de alguno de los elementos del hardware que los compone.

Las vulnerabilidades de un sistema informático son motivo de problemas constantes, ya que se hace público las debilidades de seguridad. En este sentido, existe una especie de puja por dar a conocer vulnerabilidades de un sistema de un competidor, lo que agrava la situación de todos los usuarios, ya que al quedar expuesto el problema de seguridad tan abiertamente, es aprovechado incluso por hackers y ciberdelincuentes que todavía no lo conocían.

Así mismo, clasificar las vulnerabilidades en crítica, importante, moderada y baja, permite enumerar los peligros de acuerdo con el grado de daño que puede ocasionar

FUENTES DE AMENAZAS MÁS COMUNES EN EL ÁMBITO DE SISTEMAS DE INFORMACIÓN

En línea con la identificación de estas debilidades, se debe considerar las fuentes más comunes de amenazas que se presentan en los sistemas de información como lo son:

- ✓ Malware o código malicioso: permite realizar diferentes acciones a un atacante. Desde ataques genéricos mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivos, configuración o componente específico de la red.

- ✓ Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques o para su venta.

- ✓ APT o Amenazas Persistentes Avanzadas (*Advanced Persistent Threats*): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.

- ✓ Botnets: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.

- ✓ Redes sociales: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.

- ✓ Servicios en la nube: una empresa que contrate este tipo de servicios debe tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

NUEVAS VULNERABILIDADES EXPLOTADAS ACTIVAMENTE

En relación con las nuevas vulnerabilidades explotadas activamente, de acuerdo con una publicación efectuada por Ethical Hacking Consultores, el pasado 29 de agosto de 2022, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) agregó 10 nuevas vulnerabilidades explotadas activamente a su Catálogo de Explotadas Conocidas (KEV), donde incluso se incluye una falla de seguridad de alta gravedad que afecta el software de automatización industrial de Delta Electronics.

Es importante mencionar que existe un repositorio de datos de gestión de vulnerabilidades NVD (National Vulnerability Database) del gobierno de los Estados Unidos, basados en estándares. Estos datos permiten la automatización de la gestión, la medición de la seguridad y el cumplimiento. El NVD incluye bases de datos de listas de verificación de seguridad, fallas de software relacionadas con la seguridad, configuraciones erróneas, nombres de productos y métricas de impacto.

A todas las vulnerabilidades en el NVD se les ha asignado un identificador CVE (*Common Vulnerabilities and Exposures*). El CVE tiene como propósito principal el identificar de forma única las vulnerabilidades y asociar versiones específicas de las bases de código (por ejemplo, software y bibliotecas compartidas) a ellas. El uso de CVE garantiza que dos o más partes puedan hacer referencia con confianza a un identificador CVE (ID) al discutir o compartir información sobre una vulnerabilidad única.

Con base a lo anterior, se hace mención de que las explotaciones de estas debilidades de reciente publicación cuando se divulgan por primera vez se están volviendo más rápidas, esto lleva a intentos de escaneo indiscriminado y oportunistas que tienen como objetivo aprovechar la aplicación de parches.

DEFECTOS EXPLOTADOS ACTIVAMENTE AGREGADOS A LA LISTA

Entre otros defectos explotados activamente agregados a la lista están los siguientes:

Tabla 1
Defectos explotados activamente

CVE-2022-26352	Vulnerabilidad de carga de archivos sin restricciones de dotCMS
CVE-2022-24706	Vulnerabilidad de inicialización predeterminada insegura de recursos de Apache CouchDB
CVE-2022-24112	Vulnerabilidad de omisión de autenticación APISIX de Apache
CVE-2022-22963	Vulnerabilidad de ejecución remota de código de la función Spring Cloud de VMware Tanzu
CVE-2022-2294	Vulnerabilidad de desbordamiento de búfer de pila de WebRTC
CVE-2021-39226	Vulnerabilidad de omisión de autenticación de Grafana
CVE-2020-36193	Vulnerabilidad de resolución de enlace inadecuado de PEAR Archive_Tar
CVE-2020-28949	PEAR Archive_Tar Deserialización de vulnerabilidad de datos no confiables

Fuente: https://blog.ehcgroup.io

En vista de lo anteriormente mencionado, y en la posible concordancia o correspondencia de la utilización dentro de los protocolos de interfaz, gestores de código, de base de datos, tráfico, código en entornos locales de nube pública y perimetrales, red de conexión y sistemas en nuestra institución, es importante conocer que para mitigar cada vulnerabilidad se debe de hacer de forma independiente y según su tipo o relación, además de su ambiente por ejemplo Servidores de Windows, acciones correctivas de firewalls, OpenSSL, entre otros.

OBSERVACIONES EFECTUADAS POR LOS EXPERTOS

Por lo anterior, los expertos en esta temática han emitido recomendaciones generales para mantener a salvo a los usuarios y los datos que estos manejan, por lo que se debe valorar que las organizaciones practiquen las recomendaciones dadas por los fabricantes de estos productos afectados y otros que buscan resguardar la seguridad de su organización, entre las cuales se señalan:

- Monitoreo de eventos en los servicios expuestos que utilicen Apache y otros.
- Mantener actualizados todos los productos como software, sistemas operativos entre otros.
- Realizar la actualización de los firewalls de las organizaciones y ajustes en sus reglas.
- Usar solo las aplicaciones esenciales para la organización.
- Contar con herramientas administradas de antivirus.
- En caso de tener incidentes, realizar el respectivo aislamiento de los equipos afectados y comunicarse con un especialista forense.

Como se puede observar, es importante mantener la totalidad de nuestros equipos bajo directrices de actualización de forma periódica, de manera que al momento de detectarse alguna vulnerabilidad y sea lanzado un parche por los fabricantes, se pueda tener acceso a este lo más pronto posible y disminuir así el riesgo.

De igual forma, es importante evaluar los cambios a realizar de forma manual en los equipos y la afectación que estos pueden presentar, todo esto con el fin de que la productividad de los servicios brindados por nuestra organización no se vea comprometidos.

CONSIDERACIONES NORMATIVAS

Lo expuesto en el presente oficio se realiza con el fin de que se valore la información brindada y se valoren la implementación de medidas necesarias, en cumplimiento 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", a saber:

> *"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 (…).*
>
> *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 (…)".*

CONSIDERACIONES FINALES

De acuerdo con la información analizada en torno a las nuevas vulnerabilidades expuestas en el NVD, considerando que las explotaciones de estas debilidades recientes se están realizando de forma rápida aprovechando la aplicación de parches retrasados o en su defecto ante la carencia de una seguridad adecuada, es que se informa para que se tomen las medidas correspondientes para disminuir la probabilidad de materializaciones de riesgos producto de las debilidades detectadas.

Es importante mencionar que la secuencia de estos ataques a menudo es especifica e involucra web shells, criptomineros, botnets y troyanos de acceso remoto (RAT), seguidos de intermediarios de acceso inicial (IAB) que allanan el camino para el ransomware, razón por la cual es de suma importancia reforzar los mecanismos de seguridad y detección de canales de entrada de ataques, con ayuda de la actualización de la información para poder conocer el avance de las debilidades a las cuales se está expuesto en el tema de ciberseguridad.

A su vez esta Auditoria considera oportuno se valore definir en conjunto con las instancias correspondientes, una estrategia integral orientada a realizar un diagnóstico de las vulnerabilidades actuales, incluidas las nuevas mencionadas en este oficio a las que la institución podría ser objeto, definiendo su alcance, protocolo de seguridad, protección y planes de contingencia, de manera que se analicen los riesgos asociados a los diferentes tipos de debilidades de la red, sistemas, equipos, interfaces de conexión entre otros, en la que la institución podría sufrir un ataque de las mismas dimensiones como las del pasado mes de mayo de 2022 o con una mayor gravedad.

Razón por la cual, se informa sobre lo descrito, con el objetivo de que se analice la información expuesta y se refuercen los mecanismos de ciberseguridad de considerarse la posible materialización de riesgos, una vez que se hayan reestablecido los servicios tecnológicos institucionales.

En virtud de lo expuesto, se da a conocer la información descrita, con el propósito de que se someta a revisión por parte de la Administración, analizando además las recomendaciones emanadas por los expertos, de manera que se considere definir acciones específicas dentro de sus rangos de acción, entre las cuales podrían estar las de implementar los mecanismos de información y capacitación del personal en esta materia, acorde a las políticas y normas de seguridad informática de la institución. Lo anterior para coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad informática, así como de la continuidad en la prestación de los servicios.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.09.16 10:42:57 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/EGC/lbc

Anexo(1)

1. Conceptos de seguridad que se deben conocer.

C. Auditoría

ANEXO

GLOSARIO

Delta Automatización Industrial: Delta Eletronics es líder mundial en el suministro de fuentes de alimentación conmutada y uno de los principales proveedores para la gestión de energía, componentes, displays visuales, productos de red y soluciones de automatización industrial.

dotCMS: es un sistema de gestión de contenido de código abierto escrito en Java para gestionar contenido y sitios y aplicaciones basados en contenido.

Es un poderoso sistema de gestión de contenidos que simplifica las necesidades complejas y los requisitos de integración de las grandes organizaciones. Ofrece contenido a sitios web, intranets, aplicaciones móviles y cualquier aplicación basada en la web. Los equipos pueden enviar sitios web completos a CDN o servidores distribuidos geográficamente. Los flujos de trabajo totalmente personalizables se adaptan a las necesidades de tu negocio. dotCMS se integra fácilmente con sistemas de terceros, como la automatización de marketing, el comercio electrónico, los CRM y los ERP. Disponible para descarga gratuita.

Apache CouchDB: comúnmente llamada CouchDB, es un gestor de bases de datos de código abierto, cuyo foco está puesto en la facilidad de su uso y en ser "una base de datos que asume la web de manera completa"
Apache APISIX: proporciona funciones de gestión de tráfico enriquecidas como equilibrio de carga, upstream dinámico, canary release, rotura de circuitos, autenticación, observabilidad, etc.

Spring cloud de vmware tanzu: VMware Tanzu es una tecnología inherentemente multinube, por lo que ofrece la flexibilidad de ejecutar las aplicaciones modernas de Kubernetes en cualquier lugar: entornos locales, de nube pública y perimetrales.

WebRTC: es una especificación HTML5 que permite que las páginas web reproduzcan contenido de audio y video en tiempo real dentro del navegador.

Grafana: es una herramienta de código abierto para el análisis y visualización de métricas. Se utiliza frecuentemente para visualizar de una forma elegante series de datos en el análisis de infraestructuras y aplicaciones.

PEAR Archive_Tar: El nombre "TAR" se refiere a los archivos Tape ARchive y se remonta a cuando los archivos se almacenaban en unidades en cinta. TAR es una herramienta de software utilizada para recopilar varios archivos en un solo archivo, incluyendo videos e imágenes, en uno para una distribución o archivado más fáciles.

Una vulnerabilidad en la librería Archive_Tar de PEAR podría permitir a un atacante sobrescribir archivos arbitrarios en el sistema afectado mediante el envío de un archivo especialmente diseñado, debido a que la aplicación no comprueba si el fichero del archivo es un enlace simbólico al extraerlo. Se ha asignado el identificador CVE-2021-32610 para esta vulnerabilidad.

symlink races: Una carrera de enlaces simbólicos es un tipo de vulnerabilidad de seguridad de software que resulta de un programa que crea archivos de manera insegura. Un usuario malintencionado puede crear un vínculo simbólico a un archivo al que de otro modo no sería accesible.

Web Shell: Un shell web es una interfaz similar a un shell que permite acceder de forma remota a un servidor web, a menudo con fines de ciberataques. Un shell web es único en el sentido de que se utiliza un navegador web para interactuar con él.

Figura 2
Cinco conceptos de seguridad que se deben conocer

Fuente: www.incibe.com