GammaCSOC-CERT
By Gamma Ingenieros

Boletín de Ciberseguridad Semanal

Edición °0423

GAMMA INGENIEROS

TLP:GREEN

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	1	3	
MALWARE	2	1	1
BRECHAS DE SEGURIDAD		1	1
NOTICIAS DE CIBERSEGURIDAD	1	1	1
SECTOR TELCO	1		
SECTOR SALUD	1		

VULNERABILIDADES

KeePass: potencial vulnerabilidad expone claves en texto plano

investigadores de seguridad han descubierto una supuesta vulnerabilidad (discutida) que representaría una seria amenaza para los usuarios del popular administrador de contraseñas KeePass. Una falla, identificada como CVE-2023-24055, permitiría a los atacantes obtener contraseñas almacenadas en texto no cifrado. Esto sólo sucede en la configuración por defecto de la herramienta. Se debe ejecutar el workaround, es importante conocer que ya existe una PoC pública que se puede usar fácilmente.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2023/01/keepass-potencial-vulnerabilidad-expone.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-24055
- https://github.com/deetl/CVE-2023-24055

PoC exploit para la vulnerabilidad ACE en productos Apple (CVE-2023-23504)

El investigador de seguridad Adam Doupé de ASU SEFCOM ha revelado detalles de una vulnerabilidad de seguridad ya parcheada en Apple macOS, Apple Watch, iPhone, iPad y iPod que un atacante podría explotar para ejecutar código arbitrario con privilegios del kernel. CVSS: 7,5.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityonline.info/poc-exploit-for-execute-arbitrary-code-in-apple-products-cve-2023-23504-released/

- https://github.com/adamdoupe/adamd-pocs/blob/main/CVE-2023-23504/CVE-2023-23504.c **(Prueba de Concepto)**
- https://support.apple.com/es-co/HT213601

Error de seguridad de Lexmark deja miles de sus impresoras abiertas a ataques

Lexmark ha instado a sus clientes actualizar los firmwares de sus impresoras, luego de la publicación de un exploit de prueba de concepto (PoC) que permite la ejecución remota de código (RCE).

El exploit en cuestión, designado CVE-2023-23560, puede dar a los atacantes acceso a las colas de trabajos de impresión, revelar las credenciales de la red Wi-Fi y permitir el acceso a otros dispositivos en una red.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.adslzone.net/noticias/seguridad/modelos-impresoras-grave-fallo-ataque-cibernetico/
- https://www.bleepingcomputer.com/news/security/lexmark-warns-of-rce-bug-affecting-100-printer-models-poc-released/
- https://www.evisos.com.ar/noticias/error-de-seguridad-de-lexmark-deja-miles-de-sus-impresoras-abiertas-a-ataques/
- https://publications.lexmark.com/publications/security-alerts/CVE-2023-23560.pdf

Se descubre que la app Samsung Galaxy Store, es vulnerable a la instalación fraudulenta de aplicaciones

Se han descubierto dos fallos de seguridad en la aplicación Samsung Galaxy Store para Android que podrían ser explotados por un atacante local para instalar sigilosamente aplicaciones arbitrarias o dirigir a posibles víctimas a páginas web fraudulentas.

Prioridad: 2 Urgente.

Ampliar información:

- https://andro4all.com/samsung/la-tienda-de-apps-de-tu-movil-samsung-tiene-un-grave-fallo-de-seguridad-actualiza-cuanto-antes-a-la-ultima-version
- https://www.elespanol.com/elandroidelibre/noticias-y-novedades/20230123/movil-samsung-haz-ahora-mismo-no-hackeen/735926570_0.html#:~:text=Una%20vulnerabilidad%20descubierta%20en%20la,de%20apps%20que%20no%20queremos.&text=Los%20m%C3%B3viles%20Samsung%20son%20especiales,de%20apps%2C%20llamada%20Galaxy%20Store.
- https://security.samsungmobile.com/securityUpdate.smsb

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.

- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

Secuestran la infraestructura de Ransomware Hive en operación internacional

Europol informó que tomó el control de la infraestructura del grupo de Ransomware Hive en una operación internacional en la que participaron autoridades de 13 países. La acción fue coordinada por Europol junto a fuerzas de seguridad de Estados Unidos (Departamento de Justicia, FBI y el Servicio Secreto), Alemania (Policía Federal y la Policía de Reutlingen) y Países Bajos (Unidad Nacional del Crimen Tecnológico).

Prioridad: 3 Importante.

Ampliar información:

- https://www.welivesecurity.com/la-es/2023/01/27/operacion-internacional-secuestra-infraestructura-ransomware-hive/
- https://noticiasseguridad.com/malware-virus/hackeamos-a-los-hackers-el-departamento-de-justicia-y-el-fbi-eliminan-el-ransomware-hive-despues-de-pasar-meses-dentro-de-los-sistemas-de-pandillas/
- https://www.elnacional.com/mundo/ee-uu/desmantelan-hive-una-de-las-grandes-redes-de-ataques-de-ransomware-del-mundo/
- https://www.darkreading.com/vulnerabilities-threats/hive-ransomware-gang-loses-honeycomb

Microsoft bloqueará los complementos XLL de Excel para impedir la distribución de malware

Microsoft ha anunciado planes para sus clientes 365 en los que pretende bloquear automáticamente todos los archivos XLL add-in descargados de Internet para evitar ataques de phishing que se basan en este tipo de señuelos.

Prioridad: 2 Urgente.

Ampliar información:

- https://dearce.com.uy/microsoft-bloqueara-los-complementos-xll-de-excel-para-detener-la-entrega-de-malware/
- https://www.microsoft.com/en-us/microsoft-365/roadmap?filters=&searchterms=115485
- https://www.ciberseguridadlatam.com/2023/01/25/microsoft-bloqueara-los-complementos-xll-de-excel-para-impedir-la-distribucion-de-malware/

2023 el año del malware Wiper

FortiGuard Labs está rastreando activamente el malware de tipo Wiper dirigido a organizaciones ucranianas desde el comienzo del conflicto entre Rusia y Ucrania en 2022. El aumento repentino en el malware tipo Wiper comenzó a principios de año con numerosas muestras de limpiaparabrisas nuevas dirigidas a Ucrania.

Cuando hablamos de **Wiper** nos referimos a uno de los tipos de amenazas más peligrosos que podemos encontrar. Pone en riesgo la información personal, documentos y cualquier tipo de archivos que tengamos almacenados. Su objetivo no es otro que borrar el contenido que haya en una memoria o disco.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

---

Anuncios con malware en resultados de búsqueda de Google para descargar OBS, VLC, 7-Zip, CCleaner, VirtualBox, GIMP

Basándose en la creación de sitios falsos y pautando para que la página salga en los primeros resultados de búsqueda de Google, los atacantes pretenden engañar a los usuarios. Ya son varios los casos que se conocen sobre esta modalidad de ciberataque, con la que los delincuentes quieren que la persona acceda a la página y descargue un software, que en realidad es un malware. (Redline stealer, Auora, Vidar)

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.elhacker.net/2023/01/delincuentes-ponen-anuncios-malware-en-resutlados-buscador-google.html
- https://blog.segu-info.com.ar/2023/01/delincuentes-promocionan-malware-traves.html

---

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíbir las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.

- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.

BRECHAS DE SEGURIDAD

Un hacktivista aburrido que buscaba en un servidor no seguro de una aerolínea se topó con secretos de seguridad nacional, incluida la lista de "no volar" del FBI

La lista secreta de "no volar" del Centro de Detección de Terrorismo del FBI ahora es mucho menos misteriosa gracias a un hacker suizo aburrido que estaba explorando servidores no seguros en su tiempo libre.

Prioridad: 3 Importante.

Ampliar información:

- https://noticiasseguridad.com/seguridad-informatica/un-hacktivista-aburrido-que-buscaba-en-un-servidor-no-seguro-de-una-aerolinea-se-topo-con-secretos-de-seguridad-nacional-incluida-la-lista-de-no-volar-del-fbi/
- https://computerhoy.com/ciberseguridad/filtran-online-no-fly-list-estados-unidos-lista-personas-vetadas-aviones-fbi-1188908
- https://www.businessinsider.es/hacktivista-secretos-seguridad-lista-no-volar-fbi-perversa-consecuencia-estado-vigilancia-1188694

Estafa de phishing por SMS hackean los empleados de Zendesk

Zendesk afirma que como resultado del ataque los actores de amenazas tuvieron acceso a datos no estructurados de una plataforma de registro durante un mes entre el 25 de septiembre y el 26 de octubre de 2022.

Prioridad: 2 Urgente.

Ampliar información:

- https://noticiasseguridad.com/hacking-incidentes/estafa-de-phishing-por-sms-hackean-los-empleados-de-zendesk/

NOTICIAS DE CIBERSEGURIDAD

Nuevo ataque cibernético en el sector salud: comercializadora de medicamentos fue afectada

Mediante un comunicado de prensa, la comercializadora Audifarma confirmó que fue víctima de un ataque cibernético a su infraestructura tecnológica.

"Informamos al público en general, que el domingo 22 de enero de 2023, fuimos objeto de un ataque informático externo en nuestra infraestructura tecnológica. Tan pronto lo identificamos, activamos nuestros protocolos de seguridad informática dispuestos para este tipo de casos", confirmaron.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.semana.com/salud/articulo/nuevo-ataque-cibernetico-en-el-sector-salud-esta-importante-comercializadora-de-medicamentos-fue-afectada/202347/
- https://www.elcolombiano.com/colombia/hackeo-a-audifarma-empresa-que-entrega-medicamentos-a-pacientes-de-eps-NE20174328
- https://www.semana.com/tecnologia/articulo/hackeo-a-audifarma-ademas-de-largas-filas-y-demoras-en-servicios-que-otras-afectaciones-podrian-enfrentar-sus-usuarios/202302/

8 medidas de ciberseguridad que se deben implementar para asegurar las redes ipv6

El Protocolo de Internet (IP) es el protocolo que utiliza la gran mayoría de los dispositivos en red para comunicarse. La versión 6 de IP a menudo conocida como IPv6 es la versión más reciente del Protocolo de Internet (IP) y tiene muchos beneficios sobre su predecesora, la versión 4 de IP (IPv4). El espacio de direcciones proporcionado por IPv4 es insuficiente para manejar la creciente cantidad de dispositivos en red que requieren direcciones IP enrutables mientras que IPv6 ofrece un amplio espacio de direcciones pudiendo satisfacer tanto las demandas actuales como las que puedan surgir en el futuro.

Aunque IPv6 tendrá un mayor impacto en algunas tecnologías como la infraestructura de red que en otras, casi todas las piezas de hardware y software en red se verán afectadas de alguna manera. Como consecuencia de esto IPv6 tiene una amplia gama de efectos en la ciberseguridad, los cuales deben ser abordados por las empresas con sumo cuidado.

Prioridad: 2 Urgente.

Ampliar información:

- https://noticiasseguridad.com/tutoriales/8-medidas-de-ciberseguridad-que-se-deben-implementar-para-asegurar-las-redes-ipv6/

ChatGPT es una amenaza mayor para la ciberseguridad de lo que la mayoría cree

Un modelo de IA generador de lenguaje llamado ChatGPT, disponible de forma gratuita, ha conquistado Internet. Si bien la IA tiene el potencial de ayudar a los equipos de TI y seguridad a ser más eficientes, también permite que los actores de amenazas desarrollen malware.

Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2023/01/26/chatgpt-cybersecurity-threat/
- https://rpp.pe/tecnologia/mas-tecnologia/chatgpt-hackers-crean-malware-con-inteligencia-artificial-noticia-1458838
- https://cso.computerworld.es/cibercrimen/chatgpt-puede-permitir-a-los-atacantes-mejorar-sus-estafas-significativamente