GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1424

En alianza con

TD SYNNEX FORTINET

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
VULNERABIILIDADES	0	2	3
MALWARE	0	3	1
NOTICIAS DE CIBERSEGURIDAD	0	0	4

VULNERABILIDADES

Vulnerabilidad irreparable en el chip de Apple filtra claves de cifrado secretas

Un hallazgo reciente ha revelado un nuevo problema de seguridad en los chips de la serie M de Apple, que podría ser explotado para extraer claves secretas utilizadas en operaciones criptográficas. Conocida como "GoFetch", esta vulnerabilidad está vinculada a un tipo de ataque de canal lateral microarquitectónico que aprovecha una función llamada "data memory-dependent prefetcher" (DMP), dirigida específicamente a implementaciones criptográficas de tiempo constante. Esto permite la captura de datos sensibles desde la caché de la CPU. Los investigadores informaron a Apple sobre estos hallazgos en diciembre de 2023.

Prioridad: 3 Importante.

Ampliar información:

https://unaaldia.hispasec.com/2024/03/una-vulnerabilidad-irreparable-en-el-chip-de-apple-filtra-claves-de-cifrado-secretas.html

---

Vulnerabilidad en comando "Wall"

Se ha descubierto una vulnerabilidad en el comando "wall" del paquete util-linux, que forma parte del sistema operativo Linux. Esta vulnerabilidad, registrada como CVE-2024-28085 y denominada WallEscape, podría permitir que un atacante sin privilegios robe contraseñas o modifique el portapapeles de la víctima. Este problema de seguridad ha estado presente en todas las versiones del paquete durante los últimos 11 años hasta la versión 2.40, lanzada recientemente.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/03/vulnerabilidad-en-comando-wall-linux.html

---

Vulnerabilidad crítica sin parcheo en la plataforma RAY AI es explotada para la minería de criptomonedas

Investigadores de ciberseguridad advierten que los actores de amenazas están explotando activamente una vulnerabilidad "disputada" y sin parchear en una plataforma de inteligencia artificial (IA) de código abierto llamada Anyscale Ray, con el fin de aprovechar la potencia informática para la minería ilegal de criptomonedas. "Esta vulnerabilidad permite a los atacantes tomar el control de la potencia informática de las empresas y filtrar

datos sensibles", explicaron los investigadores de Oligo Security, Avi Lumelsky, Guy Kaplan y Gal Elbaz, en una divulgación el pasado martes.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/critical-unpatched-ray-ai-platform.html

---

Alertas de CISA sobre la explotación activa de fallas en productos de Fortinet, Ivanti y Nice

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) colocó tres fallas de seguridad en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) el lunes, citando evidencia de explotación activa. Las vulnerabilidades agregadas son: CVE-2023-48788 (puntuación CVSS: 9.3) - Vulnerabilidad de Inyección SQL en Fortinet FortiClient EMS, CVE-2021-44529 (puntuación CVSS: 9.8) - Vulnerabilidad de Inyección de Código en el Servicio de Nube del Administrador de Extremos de Ivanti (EPM CSA), CVE-2019-7256 (puntuación CVSS: 10.0) - Vulnerabilidad de Inyección de Comandos OS en Nice Linear eMerge E3-Series.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/03/cisa-alerts-on-active-exploitation-of.html

---

Hackers atacando activamente una vulnerabilidad en Microsoft SharePoint

CISA ha incluido una vulnerabilidad que afecta al servidor Microsoft SharePoint en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en la evidencia de explotación activa detectada en el entorno digital. Esta vulnerabilidad, identificada como

CVE-2023-24955 y con una puntuación CVSS de 7.2, constituye una grave falla de ejecución remota de código que permite a un atacante autenticado con privilegios de propietario del sitio ejecutar código arbitrario. Según Microsoft, en un ataque basado en la red, un atacante autenticado como propietario del sitio podría ejecutar código de forma remota en el servidor SharePoint. Esta vulnerabilidad fue abordada por Microsoft como parte de sus actualizaciones de Parches de mayo de 2023.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/cisa-warns-hackers-actively-attacking.html

---

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.
- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.

- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

Ataque de phishing entrega un keylogger disfrazado de aviso de pago bancario

Se ha detectado una nueva campaña de phishing que utiliza un malware de carga para distribuir un ladrón de información y keylogger conocido como Agente Tesla. Trustwave SpiderLabs informó la idenficación un correo electrónico de phishing con esta cadena de ataque el 8 de marzo de 2024. El mensaje se hace pasar por una notificación de pago bancario, instando al usuario a abrir un archivo adjunto. El archivo ("Bank Handlowy w Warszawie - dowód wpłaty_pdf.tar.gz") contiene un cargador malicioso que activa el proceso de despliegue del Agente Tesla.

Prioridad: 2 Urgente

Ampliar información:

https://thehackernews.com/2024/03/alert-new-phishing-attack-delivers.html

---

Agenda Ransomware se propaga a vCenters y ESXi a través de PowerShell Script

Desde su descubrimiento en 2022, el grupo de ransomware Agenda (también conocido como Qilin) ha estado activo y en desarrollo, rastreado por Trend Micro como Water Galura, continúa infectando a víctimas en todo el mundo, teniendo a Estados Unidos, Argentina, Australia y Tailandia entre sus principales objetivos (según datos de amenazas del sitio de filtración del actor). Mientras tanto, el ransomware Agenda se ha utilizado para atacar varias industrias, incluidas finanzas y derecho.

Prioridad: 2 Urgente.

Ampliar información:

https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html

---

El Grupo de Hacker APT28 se dirige a Europa, América y Asia en un esquema de phishing generalizado

El grupo de amenazas APT28, con vínculos en Rusia, ha sido identificado en múltiples campañas de phishing en curso. Estas campañas utilizan documentos señuelo que imitan a organizaciones gubernamentales y no gubernamentales en regiones como Europa, el Cáucaso Sur, Asia Central, América del Norte y del Sur. Los señuelos descubiertos comprenden una variedad de documentos, algunos de los cuales son internos y otros están disponibles públicamente. Además, se han identificado posibles documentos generados por actores asociados con sectores como finanzas, infraestructura crítica, ejecutivos comprometidos, seguridad cibernética y seguridad marítima.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/03/apt28-hacker-group-targeting-europe.html

---

Red de Phishing "Darcula" aprovecha RCS e iMessage para evadir la detección

Una plataforma sofisticada de phishing como servicio (PhaaS) conocida como "Darcula" ha dirigido su atención a organizaciones en más de 100 países, aprovechando una extensa red de más de 20,000 dominios falsificados para facilitar ataques a gran escala por parte de ciberdelincuentes. Netcraft señaló: "El uso de iMessage y RCS en lugar de SMS para enviar mensajes de texto tiene el efecto secundario de evadir los firewalls de SMS, estrategia que está siendo empleada con éxito para dirigirse al Servicio Postal de los Estados Unidos

(USPS), así como a servicios postales y otras organizaciones establecidas en más de 100 países".

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/darcula-phishing-network-leveraging-rcs.html

---

Recomendaciones generales sobre Malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.
- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

El error de Microsoft Edge podría haber permitido a atacantes instalar silenciosamente extensiones maliciosas

Se podría haber aprovechado una vulnerabilidad de seguridad, que ahora ha sido parcheada, en el navegador web Microsoft Edge para instalar extensiones arbitrarias en los sistemas de los usuarios y llevar a cabo acciones maliciosas. "Esta falla podría haber permitido a un atacante explotar una API privada, inicialmente destinada a fines de marketing, para instalar de forma encubierta extensiones de navegador adicionales con amplios permisos sin el conocimiento del usuario.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/microsoft-edge-bug-could-have-allowed.html

---

Ransomware como servicio y la extraña economía de la Dark Web

El panorama del ransomware está experimentando cambios rápidos. En los últimos tres meses, se han producido eventos significativos en el ecosistema del ransomware, que incluyen la eliminación del blog de ransomware de LockBit, la salida de BlackCat y la aparición de varios grupos de ransomware más pequeños. El propósito de este artículo es proporcionar contexto sobre estas noticias recientes.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/ransomware-as-a-service-and-the-strange-economic s-of-the-dark-web/

Los nuevos resultados de búsqueda de IA de Google promueven sitios que contienen Malware y estafas

Los nuevos algoritmos de 'Experiencia generativa de búsqueda' impulsados por IA de Google están recomendando sitios fraudulentos que redirigen a los visitantes a extensiones no deseadas de Chrome, obsequios falsos de iPhone, suscripciones de spam del navegador y estafas de soporte técnico.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/google/googles-new-ai-search-results-promotes-sites-pushing-malware-scams/

Microsoft lanza una solución de emergencia para fallas de Windows Server en actualizaciones de marzo

Microsoft ha lanzado actualizaciones de emergencia fuera de banda (OOB) para abordar un problema conocido que causa bloqueos en los controladores de dominio de Windows después de instalar las actualizaciones de seguridad de Windows Server del 13 de marzo de 2024. Según lo informado por BleepingComputer el miércoles, muchos administradores de sistemas han señalado desde el martes que los servidores se congelan y reinician inesperadamente debido a una pérdida de memoria en el proceso del Servicio del subsistema de la autoridad de seguridad local (LSASS).

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/03/microsoft-lanza-una-solucion-de.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&utm_content=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&lctg=1417
