GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1124

En alianza con

TD SYNNEX FORTINET

BOLETÍN DE CIBERINTELIGENCIA DE AMENAZAS

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	1	0	1
MALWARE	0	2	2
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

La actualización de Android de marzo de 2024 corrige vulnerabilidades críticas

Las actualizaciones de seguridad reveladas para Android, abordan un total de 38 vulnerabilidades, entre las cuales se destacan dos problemas de gravedad crítica identificados en el componente del sistema.

Prioridad: 3 Importante.

Ampliar información:

https://www.cisa.gov/news-events/alerts/2024/02/15/cisa-adds-two-known-exploited-vulnerabilities-catalog

VMware corrige fallas críticas en ESXi, Workstation, Fusion y Cloud Foundation

VMware ha abordado cuatro vulnerabilidades (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255) en sus productos ESXi, Workstation, Fusion y Cloud Foundation. Algunas de estas vulnerabilidades podrían permitir a los atacantes evadir el sandbox y ejecutar código en la máquina host. Es importante destacar que VMware ESXi es un hipervisor independiente del sistema operativo, mientras que VMware Workstation y Fusion son hipervisores de escritorio. Por otro lado, VMware Cloud Foundation se presenta como una plataforma de nube híbrida. Específicamente, las CVE-2024-22252 y CVE-2024-22253 afectan a VMware ESXi, Workstation y Fusion, considerándose como críticas en términos de su potencial de explotación.

Prioridad: 1 Crítico.

Ampliar información:

https://www.helpnetsecurity.com/2024/03/07/cve-2024-22252-cve-2024-22253

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

Correos electrónicos sobre seguros de automóviles para infección NetSupport RAT

Desde finales de enero de este año, se ha detectado una campaña de correo electrónico de temática financiera y seguros de automóviles, aunque relativamente pequeña en alcance. Estos correos electrónicos maliciosos, de naturaleza básica, ofrecen al usuario una considerable suma de dinero a través de un enlace de marketing incrustado o un anuncio de Google, con la promesa de acceder a él. Sin embargo, estos enlaces conducen a sitios web comprometidos, lo que representa una amenaza potencial para la seguridad del usuario.

Prioridad: 3 Importante.

Ampliar información:

https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat

El regreso fallido de lockBit 3.0 pone en evidencia el riesgo imperecedero de la fuga de datos basada en Torrents

A fines de febrero, el grupo de ransomware LockBit 3.0, ya bajo presión, amenazó con hacer públicos documentos judiciales vinculados al expresidente de Estados Unidos, Donald Trump. Estos documentos fueron comprometidos durante el hackeo del 29 de enero al condado de Fulton en Georgia, a menos que el condado pagara un rescate antes del 2 de marzo. Es crucial destacar que esta amenaza llegó justo después de la Operación Cronos, una acción policial internacional que desmanteló la infraestructura en línea y el sitio web utilizado por las víctimas de LockBit 3.0 el 20 de febrero.

Prioridad: 2 Urgente.

Ampliar información:

https://www.resecurity.com/blog/article/lockbit-30s-bungled-comeback-highlights-the-undying-risk-of-torrent-based-data-leakage

---

Los servidores de Ransomware ALPHV/BlackCat se caen

Las actividades del grupo de ransomware ALPHV/BlackCat parecen haberse detenido abruptamente en medio de acusaciones de fraude dirigidas hacia un afiliado involucrado en el ataque a Optum, que tenía como objetivo la plataforma Change Healthcare, provocando una pérdida de 22 millones de dólares. Durante el fin de semana, se confirmó el cierre de los sitios de negociación asociados con las actividades de ransomware, lo que sugiere un posible desmantelamiento deliberado de la infraestructura. Sin embargo, el motivo exacto detrás de este cierre sigue siendo desconocido.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/alphvblackcat-gang-shuts-servers/

Nuevo malware Fakext ataca a bancos latinoamericanos

Aprovechando las características favorables de los complementos para navegadores web, un atacante puede apalancar atributos como persistencia, instalación sin fisura, privilegios elevados y exposición de datos sin cifrar para distribuir y operar troyanos bancarios. En noviembre de 2023, investigadores de seguridad de IBM Security Trusteer encontraron un nuevo malware extendido llamado Fakext que utiliza una extensión maliciosa de Edge para realizar ataques de hombre en el navegador y de inyección en la web.

Prioridad: 2 Urgente.

Ampliar información:

https://securityintelligence.com/posts/fakext-targeting-latin-american-banks/

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

Los Actores de Amenazas Hackearon Chunghwa Telecom, con Sede en Taiwán

En ScreenConnect, también hemos abordado nuestro descubrimiento sobre grupos de actores de amenazas, incluyendo las bandas Black Basta y Bl00dy Ransomware, que están explotando activamente las vulnerabilidades.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/159918/data-breach/chunghwa-telecom-data-breach.html

---

Riesgos inmediatos de la IA y sus posibles peligros del mañana

La inteligencia artificial ha ampliado significativamente el alcance y la eficacia de los ataques cibernéticos. Específicamente, los ataques de phishing, smishing y vishing han experimentado un impacto considerable con la introducción de ChatGPT y otros modelos de lenguaje avanzados. Además, la proliferación de variantes maliciosas de estos modelos, como FraudGPT, WormGPT, DarkBARD y White Rabbit, ha facilitado a los actores de amenazas la creación de código malicioso, la generación de páginas y mensajes de phishing, la identificación de vulnerabilidades y fugas, así como el desarrollo de

herramientas de piratería. Este aumento en la sofisticación y accesibilidad de las herramientas cibernéticas alimentadas por IA plantea desafíos significativos para la ciberseguridad y subraya la necesidad de medidas proactivas para proteger la información y los sistemas contra estas amenazas en evolución.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/03/08/ai-attacks/
