GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2424

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

VULNERABILIDADES

Vulnerabilidad Zero-Day en Check Point VPN

Check Point ha emitido parches para una vulnerabilidad Zero-Day utilizada en ataques para obtener acceso remoto a firewalls y penetrar redes corporativas a través de sus VPN. La empresa advirtió sobre estos ataques el lunes y compartió recomendaciones para proteger los dispositivos. La vulnerabilidad, identificada como CVE-2024-24919, permite a los atacantes leer información en Check Point Security Gateways con VPN de acceso remoto o software Blades de acceso móvil habilitados.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/05/vulnerabilidad-zero-day-en-check-point.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=205608146

Bypass de autenticación y vulnerabilidad de deserialización CVE-2024-4358

Progress, tras publicar un aviso sobre una vulnerabilidad de deserialización con CVSS 9.9, que requería autenticación, se descubrió un bypass de autenticación después de la ejecución de una actualización. Sin embargo, los intentos de explotar la vulnerabilidad de deserialización resultaron fallidos, frustrando los esfuerzos de los atacantes por aprovechar la situación.

Prioridad: 2 Urgente.

Ampliar información:

https://summoning.team/blog/progress-report-server-rce-cve-2024-4358-cve-2024-1800/

Vulnerabilidad de inyección de comandos en EmailGPT CVE-2024-5184

El Centro de Investigación en Ciberseguridad de Synopsys (CyRC) ha revelado la existencia de vulnerabilidades de inyección de comandos en el servicio EmailGPT, una API y extensión de Google Chrome, diseñada para ayudar a los usuarios a redactar correos electrónicos dentro de Gmail mediante modelos GPT de OpenAI, este servicio de API puede ser

manipulado por usuarios maliciosos para inyectar comandos directos y asumir el control de la lógica del servicio.

Prioridad: 3 Importante.

Ampliar información:

https://www.synopsys.com/blogs/software-security/cyrc-advisory-prompt-injection-emailgpt.html

---

Vulnerabilidad de inyección de argumentos en PHP 5.x para Windows CVE-2024-4577

Se ha descubierto una nueva vulnerabilidad de ejecución remota de código (RCE) en PHP/PHP-CGI para Windows, afectando a todas las versiones desde la 5.x. Se han identificado indicadores de compromiso (IOC) y exploits disponibles. El equipo de mantenimiento de PHP lanzó un parche para abordar esta vulnerabilidad. El descubrimiento fue realizado por el investigador principal de seguridad de Devcore, Orange Tsai (alias @orange_8361), quien informó del hallazgo a los desarrolladores de PHP. La vulnerabilidad afecta a todas las versiones de PHP en sistemas operativos Windows, incluyendo PHP 8.3 < 8.3.8, PHP 8.2 < 8.2.20, y PHP 8.1 < 8.1.29.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/06/vulnerabilidad-de-inyeccion-de.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

Actualizaciones falsas de navegadores distribuyen BitRAT y Lumma Stealer

Recientemente, una entidad de ciberseguridad ha descubierto ataques significativos, incluyendo el breach de Kaseya MSP y el malware more_eggs. Su labor ha sido crucial para identificar y enfrentar estas amenazas, demostrando su experiencia en la protección contra ciberataques. La detección de estos eventos resalta la importancia de contar con equipos especializados y vigilantes en el campo de la seguridad informática; subrayando la necesidad de mantener la vigilancia constante y la respuesta ágil ante posibles amenazas cibernéticas.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/beware-fake-browser-updates-deliver.html

---

Ciberdelincuentes usan kit de phishing V3B LilacSquid

Resecurity ha descubierto un grupo de ciberdelincuentes que suministra kits de phishing altamente sofisticados dirigidos a clientes bancarios en la Unión Europea. Estos kits tienen como objetivo principal interceptar datos sensibles, como credenciales y códigos OTP. Los atacantes utilizan diversas estrategias de ingeniería social para engañar a las víctimas y obtener su información privada. El hecho de que estos kits operen bajo el modelo de Phishing como Servicio (PhaaS) los hace fácilmente accesibles para el auto-alojamiento, lo que representa una amenaza significativa para la ciberseguridad.

Prioridad: 3 importante.

Ampliar información:

https://www.resecurity.com/blog/article/cybercriminals-attack-banking-customers-in-eu-with-v3b-phishing-kit

---

RAT sofisticado apunta a proyectos Gulp en NPM

La plataforma automatizada de detección de riesgos de Phylum ha detectado una publicación sospechosa en la plataforma NPM. Se trata del paquete llamado "glup-debugger-log", el cual fue publicado con dos archivos ofuscados que operaban de manera conjunta. Uno de estos archivos servía como un tipo de iniciador inicial, estableciendo el escenario para una campaña de malware al comprometer la máquina objetivo si cumplía

ciertos requisitos específicos. Posteriormente, este script descargaba componentes de malware adicionales.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/researchers-uncover-rat-dropping-npm.html

---

"Lost In The Fog" Una Nueva Amenaza de Ransomware

Arctic Wolf Labs comenzó a supervisar la propagación de una nueva variante de ransomware denominada Fog. Esta actividad de ransomware se detectó en varios casos de respuesta a incidentes de Arctic Wolf, todos ellos mostrando características similares. Todas las organizaciones afectadas pertenecen a Estados Unidos, con un 80% pe del sector educativo y un 20% del sector recreativo.

Prioridad: 2 Urgente.

Ampliar información:

https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat/

Ransomware INC Amenaza en Linux

El equipo de investigación de SonicWall Capture Labs ha llevado a cabo un exhaustivo análisis de una muestra de ransomware específicamente diseñada para sistemas Linux. Esta variante de ransomware, identificada como INC Ransomware, ha estado en circulación y actividad desde hace alrededor de un año, siendo detectada por primera vez en ese período. Su presencia continua plantea preocupaciones adicionales sobre la

seguridad cibernética en entornos Linux y resalta la importancia de una protección proactiva contra estas amenazas emergentes.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/06/inc-ransomware-the-latest-linux-threat/

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.

Revelan en Telegram listas combinadas de 361 millones de direcciones de correo

Recientemente, se compartieron 122 GB de datos de Telegram con Troy Hunt, de HaveIBeenPwned. Los datos contienen 361 millones de direcciones de correo electrónico, de las cuales 151 millones son nuevas para HIBP. Estas filtraciones, descubiertas en Telegram, son conocidas como "combolists" y se utilizan en ataques de relleno de credenciales. Su disponibilidad en HIBP subraya los riesgos de seguridad en línea.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/06/listas-combinadas-de-361-direcciones-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=205608146

Capturan a hacker con un arsenal tecnológico en Yopal

La Policía Nacional y el Gaula Militar han desarticulado una red de ciberdelincuentes en Colombia al capturar a un pirata informático conocido como "El Hacker". Este individuo estaba a punto de perpetrar un importante robo a varias cuentas bancarias del país. Tras meses de investigación, las autoridades ubicaron a este individuo, quien aparentemente comenzó su actividad delictiva en Bucaramanga y había obtenido una amplia base de datos de usuarios y empresas para llevar a cabo sus crímenes cibernéticos.

Prioridad: 3 Importante.

Ampliar información:

https://www.infobae.com/colombia/2024/06/03/iba-a-vaciar-cuentas-bancarias-y-robarse-2000-millones-en-yopal-capturan-a-hacker-con-un-arsenal-tecnologico/

Hackeada Ticketmaster, empresa que vende las entradas de Taylor Swift

Ticketmaster, la plataforma de venta de entradas de Taylor Swift, fue hackeada, exponiendo datos de 560 millones de clientes. Live Nation confirmó la actividad no autorizada después de que el grupo ShinyHunters afirmara haber robado información personal, incluyendo nombres, direcciones y detalles de tarjetas de crédito. La brecha, una de las mayores del año, fue revelada cuando un usuario ofreció vender 1,3 TB de datos por $500,000 en un foro de cibercrimen.

Prioridad: 3 Importante.

Ampliar información:

https://unaaldia.hispasec.com/2024/06/hackeada-ticketmaster-la-empresa-que-vende-las-entradas-de-taylor-swift.html

---

Emcali Bloqueó ataque cibernético

Emcali, empresa pública de Cali, se enfrentó a un ataque cibernético el domingo por la mañana, el cual, amenazó sus sistemas comerciales y de facturación. El ataque, contenido en menos de dos horas por profesionales de tecnología, evitó un problema mayor para la ciudad. Según el gerente de Emcali, Roger Mina, el ataque parecía estar dirigido a los sistemas de información comerciales, las investigaciones continúan.

Prioridad: 3 Importante.

Ampliar información:

https://www.semana.com/nacion/cali/articulo/emcali-logro-en-tiempo-record-bloquear-gran-ataque-cibernetico-como-lo-hicieron-detalles-de-una-operacion-de-alto-nivel/202442/