GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3423

En alianza con

TD SYNNEX FORTINET

BOLETIN 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	4	3	
MALWARE	2	4	
BRECHAS DE SEGURIDAD			1
NOTICIAS DE CIBERSEGURIDAD	1	5	2

VULNERABILIDADES

Código de explotación publicado para un defecto de seguridad de gravedad crítica de VMware

Se revela la publicación de código de explotación para una vulnerabilidad crítica en los productos de VMware. Esta vulnerabilidad permite a los atacantes eludir la autenticación SSH y acceder a la interfaz de línea de comandos de Aria Operations for Networks. El investigador Sina Kheirkhah destaca que la causa radica en el olvido de VMware al regenerar las claves SSH. Se destaca la urgencia de que los administradores de redes apliquen los parches de seguridad proporcionados por VMware para proteger sus sistemas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/exploit-code-published-for-critical-severity-vmware-security-defect/

Vulnerabilidad en el complemento de migración de WordPress expone los sitios web a ataques

Una vulnerabilidad en extensiones del popular plugin All-in-One WP Migration para WordPress podría exponer sitios web a ataques que divulguen información sensible. La falla, identificada como CVE-2023-40004, afecta extensiones como Box, Google Drive, OneDrive y Dropbox, permitiendo que atacantes no autenticados manipulen tokens de acceso y accedan a datos confidenciales o realicen restauraciones maliciosas. Se recomienda a los usuarios actualizar a las últimas versiones de estas extensiones para proteger sus sitios.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/vulnerability-in-wordpress-migration-plugin-exposes-websites-to-attacks/

Fallos recientes de Juniper encadenados en ataques tras la publicación del exploit PoC

Varios actores de amenazas han comenzado a explotar cuatro vulnerabilidades recientemente parcheadas en el componente J-Web de Juniper Networks' Junos OS, tras la publicación de código de explotación de prueba de concepto (PoC) en línea. Estas vulnerabilidades, catalogadas con un nivel de gravedad media, permiten a los atacantes tomar control de variables de entorno de manera remota y cargar archivos arbitrarios sin necesidad de autenticación. Aunque Juniper Networks ha emitido parches para resolver estas vulnerabilidades, la explotación ya ha comenzado, lo que

subraya la importancia de que los administradores actualicen sus sistemas afectados y estén atentos a posibles intentos de intrusión.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/recent-juniper-flaws-chained-in-attacks-following-poc-exploit-publication/

Vulnerabilidades de corrupción de memoria de alta gravedad parcheadas en Firefox y Chrome

Mozilla y Google han lanzado actualizaciones importantes para Firefox y Chrome para abordar varias vulnerabilidades de alta gravedad. Firefox 117 soluciona 13 vulnerabilidades, incluyendo cuatro de corrupción de memoria que podrían llevar a bloqueos potencialmente explotables. También se ha parcheado un desbordamiento de entero en Firefox para Windows. Por su parte, Google ha lanzado una actualización para Chrome que resuelve una vulnerabilidad de "uso después de liberar" en MediaStream, un problema que podría permitir la ejecución remota de código si se combina con otras vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/high-severity-memory-corruption-vulnerabilities-patched-in-firefox-chrome/

Múltiples fallas empresariales de Splunk permiten a los atacantes ejecutar código arbitrario

Splunk Enterprise ha corregido múltiples vulnerabilidades que abarcan desde Cross-Site Scripting (XSS) hasta ejecución remota de código. Estas vulnerabilidades afectaron a varias versiones del software y tenían un rango de gravedad de medio a alto. Se recomienda a los usuarios de Splunk Enterprise que actualicen a las versiones corregidas para proteger sus sistemas.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/multiple-splunk-enterprise-flaws/

Múltiples fallas en switches ArubaOS permiten a los atacantes ejecutar código remoto

ArubaOS-Switch, propiedad de Aruba Networks, ha corregido múltiples vulnerabilidades, incluyendo Cross-Site Scripting (XSS) almacenado, Denegación de Servicio (DoS) y corrupción de memoria. Las vulnerabilidades afectaron a varios modelos de switches Aruba Networking y se han asignado puntajes de gravedad que van de Medio a Alto. Se recomienda a los usuarios actualizar a las versiones corregidas y seguir las recomendaciones de seguridad de Aruba para minimizar los riesgos.

Prioridad: 1 Critico.

Ampliar información:

- https://gbhackers.com/multiple-flaws-arubaos-switches/

Fallo de escalada de privilegios de Microsoft Edge: ¡actualice ahora!

Microsoft Edge ha publicado una actualización de seguridad para abordar una vulnerabilidad de escalada de privilegios de alta gravedad (CVE-2023-36741) en versiones anteriores a la 116.0.1938.62. Esta vulnerabilidad requiere interacción del usuario para ser explotada por atacantes remotos y

actualmente no tiene código de explotación conocido. Aunque los detalles son limitados, Microsoft señala que afecta a la confidencialidad, integridad y disponibilidad de la aplicación y su entorno.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/microsoft-edge-privilege-escalation-flaw/

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

Colaboración Internacional Revela la Amenaza de Malware Android 'Chisel

Con la rápida evolución de las amenazas cibernéticas, el malware para Android está creciendo alarmantemente. CISA, junto con otras agencias de seguridad, ha informado sobre el malware "Chisel" que roba datos y monitorea actividades en dispositivos Android. Este malware se dirige especialmente a dispositivos utilizados por el ejército ucraniano y tiene capacidades como el acceso no autorizado y la recopilación de información. Los analistas vinculan a Chisel con la inteligencia rusa. Las recomendaciones incluyen revisar el informe de análisis, utilizar soluciones antivirus sólidas y estar alerta a posibles compromisos del sistema.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/chisel-android-malware/

Malware Bad Bazaar ataca a usuarios de Android a través de aplicaciones de Signal y Telegram armadas

El malware Android BadBazaar se está propagando a través de Google Play, la tienda Samsung Galaxy y sitios web falsos que imitan aplicaciones como Signal Plus Messenger y FlyGram. Estas campañas están relacionadas con la organización APT china GREF y tienen como objetivo a los uigures y otras minorías turcas. BadBazaar roba información del dispositivo y espía conversaciones de Signal, mientras que FlyGram también se ha observado en canales de Telegram uigures. Las principales víctimas se encuentran en países como Alemania, Polonia, EE. UU., Ucrania y otros. Ambos malwares se hacen pasar por aplicaciones legítimas para robar datos y espiar a los usuarios.

Prioridad: 1 Critico.

Ampliar información:

- https://gbhackers.com/badbazaar-malware-via-google-play/

SapphireStealer: Un Malware de Robo de Información Basado en .NET

Se ha descubierto SapphireStealer, un malware de robo de información de código abierto que se utiliza para robar datos sensibles, como credenciales corporativas. Su código fuente gratuito ha dado lugar a múltiples variantes y dificulta su detección. También se ha identificado un descargador de malware .NET llamado FUD-Loader utilizado para distribuir herramientas de administración remota. Este descubrimiento se suma a otro malware similar llamado Agniane Stealer, que se vende por $50 al mes en la dark web y se utiliza para robar credenciales y datos de criptomonedas. Los ciberdelincuentes siguen evolucionando estos malwares para llevar a cabo ataques maliciosos.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/08/sapphirestealer-malware-gateway-to.html

---

Troyano MMRat para Android ejecuta un fraude financiero remoto mediante una función de accesibilidad

Se ha detectado un nuevo troyano bancario para Android denominado MMRat que está afectando a usuarios en el sudeste asiático. Este malware tiene la capacidad de robar información y tomar control remoto de los dispositivos, y se destaca por su uso de un protocolo de comunicación personalizado para transferir datos de manera eficiente. Se propaga a través de sitios web de phishing que simulan ser tiendas de aplicaciones legítimas, a menudo haciéndose pasar por aplicaciones gubernamentales o de citas. Para protegerse, se recomienda a los usuarios que descarguen aplicaciones únicamente desde fuentes oficiales y que revisen detenidamente los permisos solicitados por las aplicaciones antes de instalarlas.

Prioridad: 1 Critico.

Ampliar información:

- https://thehackernews.com/2023/08/mmrat-android-trojan-executes-remote.html

---

Actores de amenazas se dirigen a servidores Microsoft SQL para implementar FreeWorld Ransomware

Ciberdelincuentes están explotando servidores Microsoft SQL débilmente protegidos para distribuir ransomware y herramientas maliciosas, como Cobalt Strike, en una campaña llamada DB#JAMMER. Este ataque destaca la importancia de usar contraseñas sólidas en servicios públicos y se produce en medio de un aumento generalizado de ataques de ransomware en 2023.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/09/threat-actors-targeting-microsoft-sql.html?&web_view=true

---

Ataques de Ransomware Akira: Amenaza en Auge a las VPN de Cisco ASA sin Autenticación Multifactor

Cisco advierte sobre ataques de ransomware Akira contra dispositivos Cisco ASA SSL VPN que carecen de autenticación multifactor (MFA). Los atacantes apuntan a organizaciones sin MFA. Esto subraya la importancia de MFA para prevenir el acceso no autorizado y ataques de ransomware. Se ha detectado un aumento en la actividad de amenazas en dispositivos Cisco ASA desde marzo de 2023. Akira ransomware, activo desde marzo, ahora apunta a dispositivos VPN de Cisco. Implementar MFA es esencial para reducir el riesgo de acceso no autorizado y posibles infecciones de ransomware.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/150157/cyber-crime/cisco-asa-ransomware-attacks.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.

BRECHAS DE SEGURIDAD

Hackearon información del estudio jurídico Guyer & Regules y piden rescate; la empresa ya presentó la denuncia

El estudio de abogados Guyer y Regules fue víctima de un ciberataque por parte del grupo de ransomware Lockbit. Los atacantes lograron infiltrarse en la empresa y robar una gran cantidad de datos confidenciales de clientes, que pesaban cerca de un terabyte. Posteriormente, Lockbit exigió un rescate de 300,000 dólares a cambio de la información robada, con un plazo límite para el 31 de agosto. Guyer y Regules confirmaron el ataque y declararon haber tomado medidas inmediatas,

incluyendo investigaciones forenses y denuncias a las autoridades. La situación aún se encuentra en desarrollo, y la empresa está trabajando para determinar el alcance completo del ataque y proteger a sus clientes afectados.

Prioridad: 3 Importante.

Ampliar información:

- https://ladiaria.com.uy/politica/articulo/2023/9/hackearon-informacion-del-estudio-juridico-guyer-y-regules-y-piden-rescate-la-empresa-ya-presento-la-denuncia/

NOTICIAS DE CIBERSEGURIDAD

Cómo afectará la computación cuántica a la ciberseguridad

A medida que la investigación en computación cuántica avanza, crece la preocupación de que esta tecnología pueda superar la criptografía actual. Aunque la amenaza no es inminente, se han tomado medidas para anticiparla, como la legislación en EE. UU. En cualquier caso, es importante que las organizaciones se preparen para posibles cambios en la seguridad de los datos, adoptando prácticas como la segmentación de redes y la protección de datos en reposo.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/how-quantum-computing-will-impact-cybersecurity/

Desmantelamiento de la botnet Qakbot: la operación cibernética más grande jamás realizada

El FBI, en colaboración con otros países, lideró una operación para desmantelar la infraestructura del malware Qakbot, un troyano bancario sofisticado. Esta operación se centró en la interrupción de actividades de ransomware y ciberdelincuencia en siete países y llevó a la incautación de millones de dólares en criptomonedas. Qakbot había sido utilizado previamente por grupos de ransomware, como Conti y ProLock, para causar pérdidas significativas a empresas. La operación permitió al FBI neutralizar una red criminal que había infectado más de 700,000 dispositivos en todo el mundo, incluyendo 200,000 en Estados Unidos.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/dismantling-qakbot-botnet/

Técnicas de Autenticación de Correo Electrónico: SPF, DKIM y DMARC para una Comunicación Segura.

La comunicación por correo electrónico es esencial en la era digital, pero también es vulnerable a ataques como el phishing y el spam. Para defenderse de estas amenazas, se utilizan protocolos de autenticación de correo electrónico como SPF, DKIM y DMARC. Estos protocolos verifican la identidad del remitente y la integridad del mensaje, brindando una primera línea de defensa contra las amenazas de correo electrónico. Su implementación mejora la seguridad del correo y reduce el riesgo de suplantación de identidad y phishing.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/email-authentication-protocol/

Juniper Firewalls, Openfire, Cisco ASA y Apache RocketMQ bajo ataque de nuevos exploits y botnets

Se han detectado ataques activos que aprovechan vulnerabilidades en firewalls Juniper, servidores Openfire y Apache RocketMQ. Estas amenazas incluyen la botnet Kinsing y una variante de la botnet DreamBus. Además, se ha observado un aumento en los ataques contra dispositivos Cisco ASA SSL VPN para distribuir ransomware Akira. Para protegerse, es esencial mantener sistemas actualizados y utilizar medidas de seguridad como autenticación multifactor.

Prioridad: 1 Critico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/08/juniper-firewalls-openfire-cisco-asa-y.html

---

Las extensiones de Chrome pueden robar contraseñas en texto plano de sitios web

Un equipo de investigadores ha demostrado cómo las extensiones de Chrome pueden robar contraseñas en texto plano de sitios web debido a un acceso ilimitado a los datos del sitio. A pesar de las medidas de seguridad, este problema afecta al 12.5% de las extensiones en la Chrome Web Store, incluidas algunas populares. Grandes empresas como Amazon, Google y Facebook también son vulnerables. La investigación destaca la necesidad de proteger los datos sensibles en línea y resalta la importancia de utilizar contraseñas seguras.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/chrome-extensions-can-steal-plaintext-passwords-from-websites/

Investigadores lanzaron un descriptor gratuito para el ransomware Key Group.

Investigadores de EclecticIQ han lanzado una herramienta de descifrado gratuita para el ransomware Key Group (también conocido como keygroup777), permitiendo a las víctimas recuperar sus datos sin pagar rescates. La herramienta funciona para una versión específica del ransomware creada el 3 de agosto de 2023, que contenía errores criptográficos que los investigadores pudieron explotar. Es importante mencionar que esta herramienta puede no ser efectiva en todas las muestras del ransomware Key Group.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/150207/malware/key-group-ransomware-decryptor.html

---

Jpcert de japón advierte sobre la nueva técnica de ataque 'maldoc en PDF

JPCERT ha detectado una nueva táctica de ataque llamada 'MalDoc en PDF', que consiste en incrustar archivos maliciosos de Word en archivos PDF. Esto permite que los archivos, aunque tengan la estructura de PDF, se abran en Word y ejecuten macros maliciosos. Esta técnica podría evadir la detección de algunas herramientas y se necesita precaución al analizar estos archivos.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/150012/hacking/maldoc-in-pdf-attack.html

---

Botnet KmsdBot Evoluciona: Ahora Apunta a Dispositivos IoT

El equipo de Akamai Security Intelligence Response Team (SIRT) ha descubierto una nueva versión del botnet KmsdBot que ahora se dirige a dispositivos de Internet de las cosas (IoT). KmsdBot es un malware evasivo basado en Golang que se detectó por primera vez en noviembre de 2022 y se propaga a través de conexiones SSH utilizando credenciales débiles. Se ha utilizado en campañas de minería de criptomonedas y en ataques de denegación de servicio (DDoS). La nueva versión incluye soporte para el escaneo de telnet y es compatible con más arquitecturas de CPU. Además, se dirige a servidores de juegos privados, proveedores de alojamiento en la nube, y ciertos sitios gubernamentales y educativos.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/149970/cyber-crime/kmsdbot-botnet-new-version.html