GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º4223

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	4	2	
MALWARE	1	3	
NOTICIAS DE CIBERSEGURIDAD		2	2

VULNERABILIDADES

F5 advierte sobre una vulnerabilidad crítica de ejecución remota de código en BIG-IP

F5, proveedor de soluciones de seguridad y entrega de aplicaciones, alerta a sus clientes sobre una vulnerabilidad de severidad crítica en su producto BIG-IP. Identificada como CVE-2023-46747 (con una puntuación CVSS de 9,8) afecta la interfaz de gestión de tráfico de la solución, esta vulnerabilidad permite a un atacante no autenticado ejecutar código arbitrario de forma remota, tener acceso a la red del sistema BIG-IP a través del puerto de gestión y/o las direcciones IP auto asignadas o ejecutar comandos del sistema de forma arbitraria. F5 ha lanzado parches para todas las versiones afectadas de BIG-IP y se recomienda a los usuarios aplicarlos lo antes posible.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/f5-warns-of-critical-remote-code-execution-vulnerability-in-big-ip/

---

iLeakage: Nuevo Ataque que Explota Safari para Robar Datos Sensibles de Dispositivos Apple

Nueva vulnerabilidad denominada "iLeakage" que permite realizar un ataque de canal lateral especulativo en Safari para robar información sensible de dispositivos Mac, iPhones y iPads. El ataque se basa en engañar al usuario de Safari para que abra un sitio web malicioso que se superpone a otro sitio web legítimo, lo que permite a los atacantes robar información de la página legítima. La vulnerabilidad se ha informado a Apple, pero la mitigación ofrecida es inestable y no está habilitada por defecto. Aunque el ataque requiere conocimientos avanzados, plantea preocupaciones de seguridad para los usuarios de Safari en dispositivos Apple.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/ileakage-attack-exploits-safari-to-steal-sensitive-data-from-macs-iphones/

VMware advierte sobre una grave vulnerabilidad de ejecución de código remoto en vCenter Server y Cloud Foundation

VMware emitió una advertencia sobre una grave vulnerabilidad (CVE-2023-34048) que permite la ejecución remota de código en sus productos vCenter Server y VMware Cloud Foundation. La empresa publicó parches para versiones más antiguas y destacó otra vulnerabilidad de gravedad moderada (CVE-2023-34056) que puede resultar en la divulgación parcial de información. Además, se advirtió que se ha publicado código de explotación en línea para un problema de omisión de autenticación en VMware Aria Operations for Logs.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/vmware-vcenter-flaw-so-critical-patches-released-for-end-of-life-products/

Vulnerabilidad de Inyección SQL en D-LINK permite a los atacantes obtener privilegios de administrador

Se ha descubierto una vulnerabilidad de inyección SQL en el dispositivo D-Link DAR-7000 que permite a los atacantes obtener privilegios de administrador y ejecutar comandos no autorizados en los dispositivos afectados. Actualmente se está evaluando la gravedad de esta vulnerabilidad, que ha sido identificada como CVE-2023-42406. Además, se ha publicado un PoC en GitHub que demuestra cómo se puede aprovechar esta vulnerabilidad.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/d-link-sql-injection-vulnerability/

Vulnerabilidades en VMware Tools que Permiten Escalada de Privilegios

Se han descubierto dos graves vulnerabilidades en VMware Tools, que pueden permitir la escalada de privilegios en máquinas virtuales. VMware ha lanzado parches para abordar estos problemas. Se recomienda a los usuarios de productos afectados que actualicen a las últimas versiones para protegerse contra posibles amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/vmware-tools-flaw/

Mozilla Firefox corrige múltiples vulnerabilidades

La actualización de Mozilla Firefox 119 aborda once vulnerabilidades, incluyendo tres de alta severidad. Entre ellas, se destacan dos problemas de seguridad relacionados con la memoria (CVE-2023-5730 y CVE-2023-5731), que podrían permitir a un atacante ejecutar código arbitrario en el navegador. También se solucionaron siete problemas de severidad moderada y uno de baja severidad en esta actualización. Los problemas de alta severidad incluyen uno que podría permitir el "clickjacking" de sitios web. La actualización resuelve estos problemas y se recomienda a los usuarios de Firefox actualizar sus navegadores para mantenerse seguros.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/firefox-memory-corruption-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

StripedFly": El Malware Avanzado con 1 Millón de Infecciones

El malware StripedFly, disfrazado como un minero de criptomonedas, ha pasado inadvertido durante cinco años, infectando más de un millón de dispositivos. Este malware altamente sofisticado comparte similitudes con herramientas vinculadas a la Agencia de Seguridad Nacional de los Estados Unidos y presenta una amplia gama de capacidades, incluyendo la minería de Monero, espionaje y ransomware. A pesar de su detección en 2017, su uso de técnicas avanzadas de evasión y su capacidad de propagarse de manera silenciosa han permitido que siga siendo una amenaza persistente no detectada.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/advanced-stripedfly-malware-with-1-million-infections-shows-similarities-to-nsa-malware/

Campaña Maliciosa Utiliza Mensajes de LinkedIn para Ataques de Robo de Identidad con Malware DuckTail

Un informe de la firma de ciberseguridad Cluster25, destaca una campaña maliciosa que utiliza mensajes de LinkedIn para realizar ataques de robo de identidad. Los atacantes envían mensajes desde cuentas de LinkedIn hackeadas con archivos PDF que parecen ser ofertas de trabajo, pero en

realidad enlazan a sitios web peligrosos que buscan robar datos. Esta campaña utiliza un malware llamado DuckTail, que puede tomar el control de cuentas de Facebook Business. La amenaza radica en la capacidad del malware para robar información y apuntar a cuentas de Facebook Business, lo que hace que los usuarios de LinkedIn deban ser cautelosos al abrir archivos y enlaces de fuentes desconocidas y usar software antivirus para proteger sus dispositivos.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/ducktail-malware-linkedin/

Troyano Android Rusty Droid RAT se Hace Pasar por Chrome

Un nuevo troyano para Android llamado Rusty Droid RAT se camufla como el navegador Chrome, solicitando permisos de accesibilidad para robar datos de usuarios y enviarlos a servidores controlados por ciberdelincuentes. Este malware puede interceptar mensajes SMS o correos electrónicos, actuando como un keylogger para recopilar información confidencial, incluyendo contraseñas y datos de tarjetas de crédito.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/android-malware-masquerades-chrome-browser/

Campaña de Malvertising en Brasil Distribuye el Malware GoPIX a Través de Anuncios Falsos de WhatsApp Web

Una campaña de malvertising en Brasil utiliza anuncios maliciosos relacionados con "WhatsApp web" para engañar a las víctimas y distribuir el malware GoPIX. Este malware se descarga según la configuración de puertos en la computadora del usuario y actúa como un ladrón de portapapeles,

robando solicitudes de pago PIX y reemplazándolas con información controlada por los atacantes. La campaña apunta a personas que buscan aplicaciones de mensajería y otros servicios en motores de búsqueda, lo que las expone a riesgos de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/10/malvertising-campaign-targets-brazils.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

La inteligencia artificial desafía a los humanos en el phishing

En una competencia de phishing entre correos electrónicos generados por inteligencia artificial (IA) y correos electrónicos humanos, los de la IA resultaron altamente persuasivos, además, se crearon en solo cinco minutos. Aunque los correos humanos superaron a los generados por IA, la diferencia fue mínima. Este estudio subraya cómo la IA se está utilizando en ataques de phishing y la importancia de la educación en ciberseguridad para contrarrestar esta tendencia.

Prioridad: 3 Importante.

Ampliar información:

- https://securityintelligence.com/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics/

Aplicaciones Maliciosas en Google Play con más de 2 Millones de Instalaciones

Más de 2 millones de dispositivos Android se han visto afectados por aplicaciones maliciosas en Google Play. Estas aplicaciones, que incluyen troyanos como FakeApp, Joker Trojans y HiddenAds, muestran anuncios intrusivos y tratan de ocultarse en los dispositivos una vez instaladas. Los usuarios corren el riesgo de suscripciones no deseadas y experiencias negativas debido a estas aplicaciones maliciosas.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/malicious-android-apps-on-google-play/

Octo Tempest ataca organizaciones para robar datos financieros

Microsoft está rastreando de cerca las actividades del grupo Octo Tempest, una organización de amenazas financieras que se ha destacado por su sofisticación en la extorsión a nivel mundial. Este grupo, que opera en inglés, emplea una variedad de tácticas, como la ingeniería social y el secuestro de tarjetas SIM, para llevar a cabo extorsiones. Comenzaron sus operaciones en 2022, centrándose en el secuestro de tarjetas SIM en telecomunicaciones y centros de atención telefónica, pero desde entonces han ampliado sus objetivos, involucrándose en servicios de ransomware. Su enfoque incluye ataques de phishing por SMS, secuestro de tarjetas SIM y sofisticadas estrategias de ingeniería social, lo que los convierte en una amenaza financiera altamente peligrosa.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/octo-tempest-attacking-organizations/

Filtración de datos en Casio: Información personal de clientes expuesta

Casio Computer Co., Ltd. se disculpa por una filtración de datos debido al acceso no autorizado a su servidor. El cual, contenía información personal de clientes que se registraron en su servicio educativo en línea "ClassPad.net", afectando a clientes tanto en Japón como en el extranjero. La compañía admitió no haber prevenido esta violación de seguridad, causada por un ataque cibernético externo que comprometió la base de datos en el entorno de desarrollo de "ClassPad.net". Aunque no se comprometieron otros activos, la filtración expuso nombres de clientes, direcciones de correo electrónico, país/región de residencia, información de compras y detalles de servicio. Casio está tomando medidas para fortalecer su seguridad técnica y revisar sus procedimientos operativos.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/casio-hacked-customers-personal-details-exposed/
