GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º0926

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

VULNERABILIDADES

VMWARE — INYECCIÓN DE COMANDOS EN ARIA OPERATIONS (CVE-2026-22719)

Broadcom ha alertado sobre una vulnerabilidad crítica de inyección de comandos en VMware Aria Operations (anteriormente vRealize Operations). El fallo, identificado como CVE-2026-22719, permite a un actor malintencionado no autenticado ejecutar comandos arbitrarios con privilegios elevados, lo que podría derivar en un compromiso total del sistema.

***Resumen técnico*:**

- *Identificador principal: CVE-2026-22719 (Asociado a VMSA-2026-0001).*
- *Severidad: 8.1 (Alta/Crítica) según la escala CVSSv3.*
- *Causa raíz: Inyección de comandos debido a una validación insuficiente durante procesos específicos del sistema.*
- *Mecanismo de falla: La vulnerabilidad es explotable de forma remota y sin credenciales, específicamente mientras se encuentra en ejecución un proceso de migración de producto asistida por soporte.*
- *Estado de explotación: Explotación activa confirmada. CISA ha incluido este fallo en su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) el 03 de marzo de 2026.*
- *Versiones afectadas: Aria Operations versiones 8.x (hasta 8.18.5) y 9.x (hasta 9.0.1), incluyendo implementaciones dentro de VMware Cloud Foundation (VCF).*

***Impacto potencial*:**

- *Ejecución Remota de Código (RCE): Un atacante puede tomar el control del appliance virtual ejecutando scripts maliciosos sin necesidad de interactuar con un usuario legítimo.*
- *Compromiso de la infraestructura de monitoreo: Al controlar Aria Operations, el atacante obtiene visibilidad sobre el rendimiento, la topología y las métricas de toda la infraestructura virtualizada de la organización.*
- *Escalada de privilegios y persistencia: El acceso inicial puede permitir al atacante crear cuentas administrativas locales o instalar backdoors para mantener el acceso a largo plazo.*
- *Movimiento lateral en el centro de datos: La posición estratégica de Aria Operations como herramienta de gestión facilita el salto hacia otros componentes críticos como vCenter o servidores de respaldo.*

Recomendaciones de mitigación:

1. *Actualización inmediata a versiones corregidas: Migrar de forma prioritaria a Aria Operations 8.18.6 o 9.0.2 (o las versiones equivalentes en bundles como VCF 5.2.3 / 9.0.2).*
2. *Aplicación del Script de Workaround: Si la actualización no es posible de inmediato, descargar y ejecutar el script aria-ops-rce-workaround.sh como root en todos los nodos de la infraestructura.*
3. *Restricción de acceso administrativo: Limitar el acceso a las interfaces de gestión de Aria Operations únicamente a redes administrativas confiables o mediante VPN, evitando su exposición directa a Internet.*
4. *Monitoreo de procesos de migración: Supervisar estrictamente los logs del sistema durante las ventanas de migración asistida por soporte, buscando ejecuciones de comandos inusuales o procesos hijos inesperados.*

Prioridad: Crítica.

Ampliar información:

- *https://www.tenable.com/plugins/nessus/300235*
- *https://knowledge.broadcom.com/external/article/430349*
- *https://socradar.io/blog/cve-2026-22719-vmware-aria-operations/*
- *https://thehackernews.com/2026/03/cisa-adds-actively-exploited-vmware.html*
- *https://www.cisa.gov/news-events/alerts/2026/03/03/cisa-adds-two-known-exploited-vulnerabilities-catalog*

CORUNA — KIT DE EXPLOITS PARA IOS (23 VULNERABILIDADES Y 5 CADENAS DE ATAQUE)

El Grupo de Inteligencia de Amenazas de Google (GTIG) ha revelado la existencia de Coruna (también conocido como CryptoWaters), un sofisticado kit de exploits diseñado para comprometer dispositivos iPhone de forma masiva y silenciosa. Este arsenal técnico, que incluye 23 exploits organizados en 5 cadenas completas, ha sido observado en una inusual trayectoria de proliferación: desde clientes de empresas de vigilancia comercial hasta grupos de espionaje rusos (UNC6353) y actores financieramente motivados en China (UNC6691).

Resumen técnico:

- *Identificador principal: Kit de exploits Coruna (incluye CVE-2024-23222, CVE-2023-43000, CVE-2023-32434, entre otros).*
- *Severidad: Crítica (Permite la toma de control total del dispositivo mediante navegación web).*
- *Causa raíz: Encadenamiento de múltiples fallos en el motor WebKit, escapes de sandbox y bypasses de mitigaciones de hardware (PAC y PPL).*
- *Mecanismo de falla: El kit utiliza un framework de JavaScript para realizar un fingerprinting del dispositivo. Si detecta una versión vulnerable, despliega de forma transparente exploits de ejecución remota de código (RCE) y escalada de privilegios.*
- *Estado de explotación: Explotación masiva detectada. Se ha utilizado en ataques de tipo watering hole contra ciudadanos ucranianos y en campañas globales de robo de criptomonedas a través de sitios financieros falsos.*
- *Versiones afectadas: Modelos de iPhone que ejecutan desde iOS 13.0 hasta iOS 17.2.1.*

***Impacto potencial*:**

- *Instalación silenciosa de spyware: El kit despliega el implante PLASMAGRID (PlasmaLoader), el cual se inyecta en procesos del sistema con privilegios de root para monitorear al usuario.*
- *Robo masivo de activos digitales: El malware tiene módulos específicos para exfiltrar frases semilla (seed phrases) y claves privadas de billeteras como MetaMask, Trust Wallet y Exodus.*
- *Exfiltración de información sensible: Capacidad para escanear imágenes en el disco en busca de códigos QR, analizar notas de Apple Memos y capturar credenciales bancarias.*
- *Vigilancia y espionaje geopolítico: Al ser utilizado por actores estatales, permite el seguimiento de objetivos específicos mediante la infección de sitios web locales de alta concurrencia.*

***Recomendaciones de mitigación*:**

1. *Actualización forzosa de iOS: Actualizar de inmediato a la versión más reciente de iOS (superior a la 17.3), ya que Apple ha parcheado las vulnerabilidades críticas utilizadas por este kit.*
2. *Activación del Modo de Aislamiento: Habilitar el Modo de Aislamiento (Lockdown Mode) en dispositivos de alto riesgo; los investigadores confirmaron que Coruna detiene su ejecución si detecta esta protección activa.*
3. *Uso de Navegación Privada: Emplear el modo de navegación privada para tareas sensibles, dado que el framework de Coruna está programado para abortar la infección en estas pestañas.*
4. *Evitar la instalación de perfiles o apps de terceros: Abstenerse de interactuar con sitios de criptomonedas no verificados o instalar aplicaciones fuera de la App Store oficial, que son los principales vectores de entrega detectados.*

Prioridad: Urgente.

Ampliar información:

- *https://www.diariobitcoin.com/tecnologia/herramientas-de-hackeo-de-nivel-gubernamental-para-iphone-ahora-circulan-entre-ciberdelincuentes/*
- *https://es.wired.com/articulos/un-potente-arsenal-para-espiar-iphones-posiblemente-pagado-por-el-gobierno-de-ee-uu-ahora-esta-en-manos-de-criminales*
- *https://www.elespanol.com/omicrono/software/20260304/pcoruna-kit-hackeo-iphone-gobierno-eeuu-ahora-usan-espias-rusos-ladrones-criptomonedasp/1003744155646_0.html*
- *https://www.threads.com/@zonaappleworld/post/DVeYPMgkUiK/estas-actualizaciones-menores-son-importantes-corrigen-errores-mejoran-la*
- *https://edr.com.mx/2026/03/04/edr-news-te-informa-coruna-ios-exploit-kit-uses-23-exploits-across-five-chains-targeting-ios-13-17-2-1/*

AIRSNITCH — EVASIÓN DE AISLAMIENTO EN REDES WI-FI (ATAQUE DE CAPA 1 Y 2)

Un grupo de investigadores de la Universidad de California y la KU Leuven presentó en el simposio NDSS 2026 una serie de técnicas denominadas AirSnitch. Este hallazgo demuestra que es posible evadir el "aislamiento de clientes" (AP Isolation), una protección fundamental en routers domésticos y empresariales diseñada para evitar que dispositivos en la misma red (como una red de invitados) se comuniquen entre sí. El fallo no rompe el cifrado WPA2/WPA3, sino que explota la gestión interna del tráfico en las capas físicas y de enlace.

***Resumen técnico*:**

- *Identificador: AirSnitch (Investigación académica NDSS 2026).*
- *Severidad: Crítica en entornos de redes compartidas o públicas.*
- *Causa raíz: Desincronización de identidad entre la Capa 1 (Física) y la Capa 2 (Enlace de Datos) del modelo OSI.*
- *Mecanismo de falla: El atacante utiliza suplantación de direcciones MAC para engañar al conmutador (switch) interno del punto de acceso (AP), logrando que el tráfico destinado a una víctima sea redirigido al dispositivo del atacante.*
- *Estado de explotación: Técnica demostrada en laboratorio sobre 11 modelos de routers comerciales de marcas líderes como Cisco, Ubiquiti, Netgear, TP-Link y ASUS, además de firmwares OpenWrt y DD-WRT.*
- *Requisito de ataque: El atacante debe estar conectado legalmente a la red Wi-Fi (conocer la contraseña o que sea una red abierta).*

***Impacto potencial*:**

- *Ataques Man-in-the-Middle (MitM) bidireccionales: Capacidad para interceptar, leer y modificar todo el tráfico de datos entre el router y el dispositivo de la víctima de forma transparente.*
- *Secuestro de sesiones y robo de credenciales: Al situarse en medio de la comunicación, el atacante puede capturar cookies de autenticación y contraseñas en sitios o servicios que no utilicen cifrado robusto de extremo a extremo.*
- *Envenenamiento de caché DNS: Posibilidad de redirigir las solicitudes de navegación de la víctima hacia sitios web fraudulentos (phishing) para robar información financiera o distribuir malware.*
- *Exposición de redes privadas desde redes de invitados: En routers donde la red de invitados comparte la misma subred o infraestructura interna que la red principal, un atacante podría saltar el aislamiento y atacar dispositivos corporativos confiables.*

Recomendaciones de mitigación:

1. *Segmentación estricta mediante VLANs: Configurar los identificadores de red (SSID) de invitados en VLANs totalmente separadas a nivel de infraestructura, lo que impide el "salto" de paquetes hacia la red principal.*
2. *Uso obligatorio de VPN en redes públicas: Implementar el uso de túneles VPN cifrados para todo el tráfico cuando los empleados se conecten desde aeropuertos, hoteles o cafeterías, neutralizando la capacidad de interceptación de AirSnitch.*
3. *Actualización de Firmware y Hardware: Aplicar los parches de seguridad de los fabricantes de routers; sin embargo, se advierte que algunos fallos sistémicos podrían requerir cambios en los chipsets físicos de futuras generaciones.*
4. *Adopción de arquitecturas Zero Trust: Tratar cada dispositivo en la red como potencialmente no confiable, implementando autenticación y cifrado en la capa de aplicación independientemente de la seguridad del Wi-Fi.*

Prioridad: Urgente.

Ampliar información:

- *https://www.q2bstudio.com/nuestro-blog/783954/descubre-como-vulnerabilidad-airsnitch-pone-en-peligro-redes-wifi-hogares-empresas-aprende-como-proteger-tu-conexion-ahora?scriptscookies=1*
- *https://enigmasecurity.cl/noticias-13232/*
- *https://www.xataka.com/seguridad/configurar-wi-fi-para-invitados-parecia-buena-idea-que-ha-aparecido-ultima-vulnerabilidad-airsnitch*
- *https://www.redeszone.net/noticias/seguridad/ataque-airsnitch-wifi-evadir-aislamiento/*
- *https://blog.segu-info.com.ar/2026/03/ataque-airsnitch-evita-el-cifrado-de-wi.html*

MALWARE

PACKAGIST — PAQUETES MALICIOSOS DE LARAVEL DESPLIEGAN RAT MULTIPLATAFORMA

Investigadores de seguridad han identificado una campaña de ataque a la cadena de suministro dirigida a desarrolladores de PHP/Laravel a través del repositorio oficial Packagist. El actor de amenazas, identificado como nhattuanbl, publicó múltiples paquetes que suplantan utilidades legítimas para infectar servidores y estaciones de trabajo con un Troyano de Acceso Remoto (RAT) altamente sofisticado y capaz de ejecutarse en Windows, macOS y Linux.

***Resumen técnico*:**

- *Paquetes identificados*: *nhattuanbl/lara-helper, nhattuanbl/simple-queue y nhattuanbl/lara-swagger.*
- *Mecanismo de infección*: *El paquete lara-swagger actúa como un "caballo de Troya" que, aunque parece inofensivo, instala automáticamente el malware lara-helper como una dependencia obligatoria.*
- *Análisis del Payload*: *El código malicioso reside en src/helper.php y utiliza técnicas avanzadas de obfuscación, incluyendo cadenas codificadas en hexadecimal/octal, obfuscación de flujo de control mediante goto e identificadores aleatorios para evadir herramientas de análisis estático.*
- *Infraestructura C2*: *Una vez activo, el RAT establece una conexión TCP con el servidor de comando y control en helper.leuleu[.]net:2096 para recibir instrucciones.*
- *Persistencia*: *El malware se reinicia automáticamente como un proceso de fondo independiente del servidor web, garantizando su ejecución continua incluso si la solicitud web original finaliza.*

***Impacto potencial*:**

- *Control total del host comprometido: El atacante obtiene una shell interactiva que permite la ejecución de comandos arbitrarios (Shell/PowerShell) con los mismos privilegios que el servidor web.*
- *Exfiltración de secretos y credenciales: Al ejecutarse en el contexto de la aplicación Laravel, el RAT tiene acceso directo a archivos de configuración críticos, incluyendo el archivo .env, contraseñas de bases de datos y llaves de API.*
- *Espionaje y captura de información: Capacidad para realizar capturas de pantalla en tiempo real mediante la función imagegrabscreen(), además de cargar o descargar archivos de manera arbitraria desde el sistema de archivos.*
- *Movimiento lateral y persistencia en la red: El acceso remoto persistente permite al atacante utilizar el servidor comprometido como punto de salto para explorar y atacar otros recursos dentro de la red interna de la organización.*

***Recomendaciones de mitigación*:**

1. *Eliminación y limpieza inmediata: Desinstalar los paquetes lara-helper, simple-queue y lara-swagger de todos los entornos. Es imperativo eliminar manualmente el archivo src/helper.php y cualquier archivo de bloqueo (lock file) residual en el directorio temporal del sistema.*
2. *Rotación exhaustiva de secretos: Cambiar de forma inmediata todas las contraseñas de bases de datos, llaves de cifrado de la aplicación, tokens de proveedores de servicios (AWS, Stripe, etc.) y cualquier credencial almacenada en el entorno comprometido.*
3. *Bloqueo y monitoreo de red: Implementar reglas de firewall para bloquear cualquier tráfico saliente hacia el dominio helper.leuleu[.]net y el puerto 2096. Auditar los logs de red en busca de conexiones históricas hacia esta infraestructura.*
4. *Auditoría de integridad del sistema: Realizar un escaneo completo de los servidores afectados para identificar scripts, procesos o cuentas de usuario inusuales creados por el RAT durante el periodo de compromiso.*

5. *Fortalecimiento del desarrollo (AppSec): Implementar herramientas de análisis de composición de software (SCA) en el pipeline de CI/CD para detectar dependencias maliciosas o vulnerables antes de que lleguen a entornos de producción.*

Prioridad: Urgente.

Ampliar información:

- *https://thehackernews.com/2026/03/fake-laravel-packages-on-packagist.html*
- *https://www.cirt.gov.jm/advisory/fake-laravel-packages-packagist-deploy-rat-windows-macos-and-linux*
- *https://cybersecurity88.com/news/fake-laravel-packages-on-packagist-deliver-cross-platform-rat-targeting-developers/*
- *https://gbhackers.com/malicious-laravel-packages/*

Recomendaciones generales sobre malware:

1. *Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.*
2. *Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.*
3. *Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.*
4. *Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.*
5. *Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.*
6. *Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.*

NOTICIAS DE CIBERSEGURIDAD

CYBERSTRIKEAI: HERRAMIENTA OFENSIVA BASADA EN IA COMPROMETE DISPOSITIVOS FORTINET A NIVEL GLOBAL

Investigadores de inteligencia de amenazas de Team Cymru y Amazon han identificado una campaña masiva de ciberespionaje que utiliza CyberStrikeAI, una plataforma ofensiva de código abierto potenciada por inteligencia artificial. Esta herramienta, desarrollada bajo el alias Ed1s0nZ y vinculada con el Ministerio de Seguridad del Estado (MSS) de China, ha sido utilizada para comprometer más de 600 dispositivos Fortinet FortiGate en 55 países en un corto periodo operativo.

Resumen técnico:

- *Naturaleza de la amenaza: CyberStrikeAI es un framework de pruebas de seguridad "nativo de IA" escrito en Go que integra más de 100 herramientas ofensivas automatizadas.*
- *Modus Operandi: A diferencia de ataques tradicionales, la campaña no explotó vulnerabilidades Zero-Day. En su lugar, utilizó IA para automatizar el escaneo de puertos de gestión expuestos y realizar ataques de fuerza bruta contra dispositivos con autenticación débil.*
- *Orquestación mediante IA: El atacante utilizó modelos de lenguaje (LLM) para generar planes de ataque paso a paso, secuencias de comandos personalizadas y metodologías de explotación adaptativas según el objetivo.*
- *Atribución técnica: El desarrollador del kit ha sido vinculado a proyectos de seguridad estatales chinos (como Knownsec 404) y recientemente intentó ocultar premios recibidos por la base de datos de vulnerabilidades del gobierno chino (CNNVD).*

***Impacto potencial*:**

- *Compromiso masivo de perímetros de red: La automatización mediante IA permite a actores con pocos conocimientos técnicos ejecutar ataques a una escala y velocidad que superan las capacidades de respuesta manuales.*
- *Acceso persistente y exfiltración de credenciales: Una vez obtenido el acceso inicial a través del puerto de gestión, los atacantes recolectan credenciales administrativas para facilitar movimientos laterales profundos en la red interna.*
- *Vigilancia estatal a gran escala: Dada la vinculación con agencias de inteligencia, el compromiso de estos dispositivos perimetrales busca establecer una infraestructura de escucha persistente sobre el tráfico cifrado de organizaciones gubernamentales y corporativas.*
- *Resiliencia ante defensas convencionales: La capacidad de la herramienta para variar sus firmas de ataque y utilizar proxies dificulta la detección basada en patrones estáticos de comportamiento.*

***Recomendaciones para mitigar el riesgo*:**

1. *Habilitación obligatoria de MFA: Implementar autenticación multifactor en todas las interfaces de gestión de red; la mayoría de los dispositivos comprometidos solo dependían de contraseñas de un solo factor.*
2. *Deshabilitar interfaces de gestión en Internet: Configurar los dispositivos FortiGate para que sus consolas administrativas no sean accesibles desde la red pública, utilizando en su lugar VPNs de administración o redes fuera de banda.*
3. *Bloqueo de indicadores de compromiso (IoC): Monitorear y bloquear el tráfico relacionado con la IP 212.11.64.250 y el puerto 8080, asociados frecuentemente con el panel de control de CyberStrikeAI.*
4. *Auditoría de logs de acceso: Realizar una revisión exhaustiva de los registros de acceso administrativo en busca de conexiones provenientes de geografías inusuales o en horarios no laborales, especialmente durante los meses de enero y febrero de 2026.*

Prioridad: Urgente.

Ampliar Información:

- *https://www.csoonline.com/article/4140221/ai-powered-attack-kits-go-open-source-and-cyberstrikeai-may-be-just-the-beginning.html*
- *https://thehackernews.com/2026/03/open-source-cyberstrikeai-deployed-in.html*
- *https://gbhackers.com/fortinet-fortigate-devices-targeted-by-cyberstrikeai/*