GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1426

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

VULNERABILIDADES

GPUBreach – ESCALADA A NIVEL CPU DESDE GPU (ROWHAMMER EN GDDR6)

Investigadores de la Universidad de Toronto han presentado GPUBreach, una evolución crítica de los ataques RowHammer que, por primera vez, demuestra cómo bit-flips en la memoria de video (VRAM) pueden derivar en un compromiso total del sistema operativo. A diferencia de ataques previos, GPUBreach no solo corrompe datos, sino que manipula las estructuras de control de la GPU para saltar al procesador central (CPU).

Resumen técnico:

- Identificadores principales: GPUBreach, GDDRHammer y GeForge.
- Severidad: Crítica (Permite la obtención de una shell de root).
- Causa raíz: Vulnerabilidad física de hardware por interferencia electromagnética en memorias GDDR6, combinada con fallos de seguridad de memoria en los controladores (drivers) de NVIDIA.
- Mecanismo de falla: Mediante el "martilleo" (hammering) de filas de memoria en la GPU, el atacante induce bit-flips en las tablas de páginas (PTE). Esto permite ganar acceso arbitrario de lectura/escritura en la VRAM, el cual se encadena con bugs en el driver de NVIDIA para realizar una escritura arbitraria en el kernel de la CPU.
- Estado de explotación: Revelado en abril de 2026; afecta incluso con la protección IOMMU activada, ya que corrompe el estado del driver dentro de buffers permitidos.
- Versiones afectadas: GPUs NVIDIA basadas en microarquitecturas Turing (Serie RTX 20), Ampere (Serie RTX 30) y Ada Lovelace (Serie RTX 40) que utilizan memoria GDDR6 y Estaciones de trabajo y servidores con modelos como la NVIDIA RTX A6000 y tarjetas de consumo que no cuentan con protección ECC robusta.

Impacto potencial:

- Escalada de privilegios a nivel de CPU: Un proceso sin privilegios puede obtener una shell de root, permitiendo el control total sobre el host afectado.
- Degradación masiva de modelos de IA: Capacidad para reducir la precisión de modelos de lenguaje (LLM) y redes neuronales del 80% al 0% mediante la manipulación sigilosa de pesos en la memoria.
- Exfiltración de llaves criptográficas: Se ha demostrado la capacidad de extraer claves secretas de la librería NVIDIA cuPQC, utilizada para acelerar la criptografía post-cuántica.
- Compromiso de entornos Cloud multi-inquilino: Los atacantes pueden romper el aislamiento entre diferentes máquinas virtuales o contenedores que comparten el mismo hardware físico de GPU

Recomendaciones de mitigación:

1. Activación obligatoria de ECC: Habilitar el Código de Corrección de Errores (ECC) en GPUs de servidor y estaciones de trabajo (ej. serie RTX A6000) para detectar y corregir bit-flips simples.
2. Actualización proactiva de drivers: Instalar los parches de seguridad de NVIDIA tan pronto sean liberados, ya que el ataque depende de vulnerabilidades específicas en el código del controlador para la escalada a CPU.
3. Restricción de ejecución de kernels CUDA: Limitar la capacidad de ejecutar código CUDA no confiable en servidores que procesan información altamente sensible o llaves criptográficas.
4. Monitoreo de telemetría de GPU: Implementar soluciones que vigilen patrones de acceso a memoria inusuales que puedan indicar un intento de ataque por martilleo de filas.

Prioridad: Crítica.

Ampliar información:

- https://www.securityweek.com/gpubreach-root-shell-access-achieved-via-gpu-rowhammer-attack/
- https://securityaffairs.com/190455/security/gpubreach-exploit-uses-gpu-memory-bit-flips-to-achieve-full-system-takeover.html
- https://www.heise.de/en/news/GPUBreach-System-takeover-with-bit-flips-in-Nvidia-GPU-11247505.html
- https://www.profesionalreview.com/2026/04/09/gpubreach-amenaza-rowhammer-gpus-nvidia/
- https://thehackernews.com/2026/04/new-gpubreach-attack-enables-full-cpu.html

CVE-2026-34040 – BYPASS DE AUTORIZACIÓN EN DOCKER ENGINE

Se ha revelado una vulnerabilidad de alta severidad en Docker Engine que permite a un atacante evadir por completo los plugins de autorización (AuthZ) mediante el envío de solicitudes HTTP manipuladas. Este fallo representa una regresión técnica de una vulnerabilidad corregida originalmente en 2024 (CVE-2024-41110), afectando al 92% de los despliegues de contenedores a nivel empresarial.

Resumen técnico:

- Identificador principal: CVE-2026-34040.
- Severidad: 8.8 (Alta) según la escala CVSS v3.1.
- Causa raíz: CWE-863 (Autorización incorrecta) debido a un manejo inconsistente de cuerpos de solicitud HTTP que exceden 1 MB.
- Mecanismo de falla: El middleware de Docker descarta silenciosamente el cuerpo de las solicitudes que superan el límite de 1 MB antes de enviarlas al plugin de autorización (como OPA o Prisma Cloud). Al recibir una solicitud aparentemente vacía, el plugin aprueba la acción, pero el demonio de Docker procesa la solicitud original completa, permitiendo la ejecución de comandos privilegiados.
- Estado de explotación: Parche publicado el 25 de marzo de 2026; se advierte que agentes de IA podrían descubrir y explotar este fallo de forma autónoma durante tareas de depuración.
- Versiones afectadas: Docker Engine; Todas las versiones desde la 1.10 (lanzada en 2016) hasta la 29.3.0. y Docker Desktop; Todas las versiones anteriores a la 4.66.1.

Impacto potencial:

- Toma de control total del host: Un atacante puede crear contenedores privilegiados con acceso irrestricto al sistema de archivos del host.
- Exfiltración de secretos críticos: Acceso directo a llaves de AWS, claves SSH, configuraciones de Kubernetes (kubeconfig) y otros datos sensibles almacenados en la máquina física.
- Bypass de políticas de seguridad corporativas: Inutilización total de herramientas de cumplimiento y gobernanza como Open Policy Agent (OPA), Casbin y Prisma Cloud.
- Explotación por agentes de IA: Herramientas automatizadas de codificación y depuración pueden construir solicitudes con "padding" para saltarse restricciones de seguridad sin intervención humana.

Recomendaciones de mitigación:

1. Actualización inmediata: Migrar urgentemente a Docker Engine 29.3.1 o Docker Desktop 4.66.1, versiones que implementan una corrección de tipo "fail-closed".
2. Configuración de Proxy Inverso: Implementar un límite de tamaño de cuerpo de solicitud (ej. 512 KB) en el gateway de la API o proxy inverso para bloquear intentos de bypass por sobrecarga.
3. Adopción de Modo Rootless: Ejecutar Docker en modo "rootless" para asegurar que, incluso en caso de compromiso, el usuario "root" del contenedor mapee a un usuario sin privilegios en el host.
4. Restricción del API de Docker: Limitar el acceso al socket de Docker únicamente a usuarios y sistemas de confianza, siguiendo estrictamente el principio de mínimo privilegio.

Prioridad: Crítica.

Ampliar información:

- https://cybersecuritynews.com/docker-vulnerability-bypass-authorization/
- https://www.cryptika.com/docker-vulnerability-let-attackers-bypass-authorization-and-gain-host-access/
- https://www.esecurityplanet.com/threats/docker-flaw-cve-2026-34040-lets-attackers-bypass-security-controls-and-take-over-hosts/
- https://thehackernews.com/2026/04/docker-cve-2026-34040-lets-attackers.html
- https://www.cyera.com/blog/cyera-research-discovers-docker-authorization-bypass-that-silently-disables-security-policies

CVE-2026-20093 – BYPASS DE AUTENTICACIÓN EN CISCO INTEGRATED MANAGEMENT CONTROLLER (IMC)

Se ha identificado una vulnerabilidad crítica en la función de cambio de contraseña del Cisco IMC, el sistema de gestión de hardware integrado en los servidores de Cisco. Este fallo permite a un atacante remoto no autenticado saltarse los mecanismos de seguridad y obtener acceso completo con privilegios de administrador, lo que representa un riesgo extremo para la infraestructura de cómputo.

Resumen técnico:

- Identificador principal: CVE-2026-20093.
- Severidad: 9.8 (Crítica) según la escala CVSS v3.1.
- Causa raíz: CWE-20 (Validación de entrada incorrecta) en el procesamiento de solicitudes de modificación de contraseña a través de la API XML del IMC.
- Mecanismo de falla: El atacante envía una solicitud HTTP POST especialmente diseñada al método configConfMo. Debido a un fallo en la validación de la sesión antes de procesar el cambio de credenciales, el sistema permite resetear la contraseña de cualquier cuenta, incluida la de administrador, sin haber iniciado sesión previamente.
- Estado de explotación: Divulgado el 1 de abril de 2026; no se reportan exploits activos en el momento de la publicación, pero el riesgo de ingeniería inversa es alto.
- Versiones afectadas: Sistemas de Cómputo: 5000 Series ENCS (NFVIS < 4.15), Catalyst 8300 Series Edge uCPE (NFVIS < 4.16), y servidores UCS C-Series M5/M6 (standalone), Servidores de Rama; UCS E-Series versiones M3 y M6.

Impacto potencial:

- Control total a nivel de hardware: Al comprometer el IMC, el atacante obtiene control sobre el servidor por debajo del sistema operativo y del hipervisor, lo que hace al ataque invisible para herramientas tradicionales como EDR.
- Manipulación de infraestructura crítica: Capacidad para apagar, encender o reiniciar servidores (power cycle), lo que puede causar denegación de servicio física y pérdida de disponibilidad de servicios críticos.
- Persistencia profunda: Un atacante puede crear cuentas de administración persistentes dentro del firmware de gestión, manteniendo el acceso incluso si se reinstala el sistema operativo del host.
- Punto de salto para movimiento lateral: El acceso al controlador de gestión puede ser utilizado para pivotar hacia otras redes de administración o capturar tráfico de red que pasa por el hardware del servidor.

Recomendaciones de mitigación:

1. Actualización prioritaria de Firmware: Instalar las versiones corregidas de Cisco IMC (ej. 4.3(2.260007) para M5 o 6.0(1.250174) para M6) y NFVIS según el modelo de hardware específico.
2. Aislamiento de la Red de Gestión: Restringir el acceso a todas las interfaces de Cisco IMC a una VLAN de gestión dedicada y aislada, bloqueando cualquier enrutamiento directo desde redes no confiables o internet.
3. Implementación de Jump Hosts y MFA: Obligar a que todo acceso administrativo pase por servidores de salto (Jump Hosts) endurecidos que requieran autenticación multifactor (MFA) obligatoria.
4. Auditoría de Cuentas y Logs: Revisar inmediatamente la lista de usuarios creados en el IMC para detectar cuentas sospechosas y monitorizar logs del SIEM en busca de solicitudes HTTP inusuales hacia los URIs de cambio de contraseña.

Prioridad: Crítica.

Ampliar información:

- https://www.helpnetsecurity.com/2026/04/03/cisco-imc-vulnerability-cve-2026-20093/
- https://socradar.io/blog/cve-2026-20093-cisco-imc-flaw/
- https://ccb.belgium.be/advisories/warning-critical-authentication-bypass-vulnerability-cisco-integrated-management
- https://www.cycognito.com/blog/emerging-threat-cve-2026-20093-cisco-imc-authentication-bypass/
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn

MALWARE

PRISMEX (VINCULADO A APT28 / FOREST BLIZZARD)

El grupo de amenazas ruso APT28 (también conocido como Pawn Storm o Fancy Bear) ha desplegado una nueva e innovadora suite de malware denominada PRISMEX. Esta campaña, detectada activamente en la primera semana de abril de 2026, destaca por su rapidez para explotar vulnerabilidades de día cero en Windows y su sofisticado uso de esteganografía para ocultar sus componentes maliciosos dentro de archivos de imagen legítimos.

Resumen técnico:

- Identificadores principales: PRISMEX (incluye PrismexSheet, PrismexDrop, PrismexLoader y PrismexStager).
- Tipo: Suite de malware para espionaje y sabotaje (Backdoor / RAT).
- Vector de ataque: Campañas de spear-phishing que utilizan archivos LNK maliciosos y la explotación encadenada de vulnerabilidades recientes (CVE-2026-21509 y CVE-2026-21513).
- Mecanismo de persistencia: Uso avanzado de COM Hijacking (secuestro de objetos COM), manipulación del registro de Windows y creación de tareas programadas.
- Comando y Control (C2): Abuso de servicios legítimos de almacenamiento en la nube, específicamente Filen.io, para evadir detecciones basadas en tráfico de red sospechoso.
- Técnica de evasión: Implementación del algoritmo "Bit Plane Round Robin" para extraer cargas útiles .NET ocultas en archivos PNG (ej. SplashScreen.png), ejecutándolas completamente en memoria para evitar dejar rastro en el disco.

Impacto potencial:

- Espionaje y exfiltración de datos: Robo sistemático de correos electrónicos a través del componente MiniDoor y acceso a documentos estratégicos en sectores de defensa y logística.
- Capacidad de sabotaje destructivo: El malware incluye comandos de tipo "wiper" capaces de borrar por completo el directorio de perfil de usuario (%USERPROFILE%), inutilizando las estaciones de trabajo.
- Compromiso de la cadena de suministro: Ataques dirigidos a socios logísticos y de apoyo militar, permitiendo a los atacantes mapear y dislocar rutas de suministro y planificación operativa.

- Control total del endpoint: El uso del framework de post-explotación COVENANT otorga a los atacantes una capacidad de ejecución de comandos remotos con alta persistencia y sigilo.

Recomendaciones de mitigación:

1. Parcheo urgente de sistemas operativos: Aplicar de forma inmediata las actualizaciones de seguridad de Microsoft para corregir CVE-2026-21513 y CVE-2026-21509, bloqueando la cadena de infección inicial.
2. Monitoreo de COM Hijacking: Implementar reglas de detección (EDR/SIEM) que vigilen la creación o modificación de CLSIDs en el registro de Windows, especialmente aquellos que apuntan a DLLs en directorios temporales o de usuario.
3. Restricción de tráfico a nubes públicas: Bloquear o inspeccionar rigurosamente el tráfico hacia servicios de almacenamiento no corporativos como Filen.io, utilizados por el malware para su comunicación C2.
4. Endurecimiento de políticas de macros y LNK: Deshabilitar la ejecución de macros de Office de origen externo y restringir el lanzamiento de aplicaciones a través de archivos .LNK recibidos por correo electrónico o desde la web.

Prioridad: Urgente.

Ampliar información:

- https://community.opentextcybersecurity.com/vulnerability-vault-228/russia-linked-apt28-uses-prismex-to-infiltrate-ukraine-and-allied-infrastructure-with-advanced-tactics-363988
- https://www.cronup.com/feed-de-noticias-de-ciberseguridad-08-04-2026/
- https://thehackernews.com/2026/04/apt28-deploys-prismex-malware-in.html

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

PROYECTO GLASSWING – IA PARA LA DETECCIÓN MASIVA DE ZERO-DAYS

Anthropic ha lanzado oficialmente el Proyecto Glasswing, una coalición estratégica que incluye a gigantes como AWS, Google, Microsoft, NVIDIA, Cisco y JPMorgan Chase. El objetivo central es el despliegue de Claude Mythos Preview, un modelo de IA de nueva generación diseñado específicamente para la defensa proactiva, capaz de identificar vulnerabilidades de día cero a una escala y profundidad sin precedentes en la historia de la ciberseguridad.

Resumen técnico:

- Motor tecnológico: Claude Mythos Preview, un modelo con capacidades de razonamiento profundo que alcanza un 93.9% en la prueba SWE-bench Verified y un 83.1% en reproducción de vulnerabilidades (CyberGym).
- Alcance del proyecto: Análisis autónomo de bases de código críticas, sistemas operativos (Linux, OpenBSD) y librerías omnipresentes como FFmpeg.
- Hallazgos históricos: Durante las pruebas iniciales, la IA detectó miles de vulnerabilidades, incluyendo un fallo de 27 años en OpenBSD y un error de 16 años en FFmpeg que había evadido millones de pruebas automatizadas tradicionales.
- Modelo de operación: Distribución controlada a través de APIs empresariales, donde los hallazgos se comunican de forma responsable a los propietarios de los sistemas antes de su divulgación pública.

Impacto potencial:

- Cambio de paradigma en la defensa: La capacidad de automatizar la investigación de seguridad de alto nivel permite cerrar brechas históricas antes de que actores malintencionados puedan explotarlas.
- Reducción drástica del "MTTD" (Mean Time To Detect): Lo que antes requería meses de auditoría manual por expertos de élite, ahora puede ser procesado en minutos por agentes de IA autónomos.
- Protección de infraestructura crítica: El fortalecimiento de sistemas base (kernels, bases de datos y redes) eleva la resiliencia de sectores estratégicos como el financiero, salud y energía.
- Equilibrio frente a amenazas de IA ofensiva: Glasswing surge como respuesta directa al uso de IA por parte de grupos estatales (como APT28) para automatizar ataques, buscando otorgar una ventaja táctica a los defensores.

Recomendaciones para mitigar el riesgo:

1. Integrar auditoría asistida por IA: Evaluar la incorporación de herramientas basadas en modelos de lenguaje avanzados en el pipeline de CI/CD para identificar errores de lógica y seguridad en etapas tempranas.
2. Elevar estándares de desarrollo: Reconocer que la "seguridad por oscuridad" o la antigüedad del código ya no son protecciones válidas; el software crítico debe someterse a revisiones profundas con estas nuevas capacidades.
3. Alinear políticas de divulgación: Revisar y actualizar los programas de Vulnerability Disclosure Policy (VDP) para manejar el posible aumento en el volumen de reportes generados por herramientas de IA.
4. Capacitación en "IA-Blue Teaming": Fomentar que los equipos de seguridad desarrollen habilidades para supervisar y validar las mitigaciones propuestas por modelos autónomos, manteniendo siempre el "human-in-the-loop".

Prioridad: Importante.

Ampliar Información:

- https://bravenewcoin.com/es/insights/anthropic-unveils-claude-mythos-and-project-glasswing-the-ai-model-too-dangerous-to-release-publicly
- https://www.securitylab.lat/news/571320.php
- https://www.diariobitcoin.com/noticias/anthropic-enciende-alarmas-con-mythos-y-glasswing-por-riesgo-de-ciberataques/
- https://ecosistemastartup.com/project-glasswing-ia-para-blindar-software-critico/