GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1726

TLP:GREEN
TRAFFIC LIGHT PROTOCOL
https://www.first.org/tlp/

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN º1726

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

CVE-2026-42208 – LITELLM (INYECCIÓN SQL CRÍTICA PRE-AUTENTICACIÓN)

Se ha detectado una vulnerabilidad de inyección SQL crítica en el proxy de IA de código abierto LiteLLM. El fallo permite a atacantes no autenticados extraer credenciales sensibles de proveedores de LLM y secretos de configuración directamente desde la base de datos PostgreSQL de la plataforma.

Resumen técnico:

- Identificador principal: CVE-2026-42208.
- Severidad: 9.3 (Crítica) según la escala CVSS v4.0.
- Causa raíz: Una falla en la verificación de claves del proxy donde el valor del token Bearer suministrado por el usuario se concatena directamente en la consulta SQL en lugar de usar consultas parametrizadas.
- Mecanismo de falla: El vector se activa antes de la fase de autenticación. Un atacante puede enviar una cabecera Authorization manipulada (ej. sk-litellm') a cualquier ruta de la API (como POST /chat/completions), forzando la ejecución de comandos SQL arbitrarios a través de la ruta de manejo de errores del proxy.
- Estado de explotación: Explotación activa detectada en la naturaleza desde el 26 de abril de 2026, aproximadamente 36 horas después de su divulgación.
- Versiones afectadas: Versiones de LiteLLM desde la 1.81.16 hasta la 1.83.6.

Impacto potencial:

- Exfiltración masiva de secretos: Robo de claves API de proveedores críticos como OpenAI, Anthropic y credenciales de AWS Bedrock almacenadas en la tabla litellm_credentials.
- Compromiso total de infraestructura cloud: Debido a que una sola fila de credenciales puede contener acceso de administrador, el impacto escala de un incidente en el proxy a un compromiso total de cuentas en la nube.
- Modificación de la base de datos: Capacidad para alterar configuraciones de entorno, variables de sistema y tablas de usuarios/equipos mediante cargas útiles de inyección SQL dirigidas.
- Consumo no autorizado y fraude financiero: Uso de los tokens exfiltrados para realizar llamadas a modelos de lenguaje de alto costo, resultando en pérdidas financieras significativas para la organización afectada.

Recomendaciones de mitigación:

1. Actualización inmediata a la versión 1.83.7: Instalar la versión estable más reciente que implementa el uso de parámetros separados para las consultas de base de datos.
2. Rotación obligatoria de credenciales: Es imperativo revocar y regenerar todas las claves de proveedores (OpenAI, Anthropic, AWS, etc.) y secretos maestros gestionados por LiteLLM tras aplicar el parche.
3. Deshabilitar registros de errores (Mitigación temporal): Configurar disable_error_logs: true en los ajustes generales para cerrar la ruta por la cual la entrada no confiable alcanza la consulta vulnerable.
4. Implementación de filtrado en el perímetro (WAF): Desplegar reglas de inspección en proxies inversos o WAF para bloquear patrones de inyección SQL (UNION, SELECT, comillas simples) en la cabecera Authorization.

Prioridad: Crítica.

Ampliar información:

- https://www.securityweek.com/fresh-litellm-vulnerability-exploited-shortly-after-disclosure/
- https://blog.elhacker.net/2026/04/vulnerabilidad-critica-de-inyeccion-sql.html#google_vignette
- https://thehackernews.com/2026/04/litellm-cve-2026-42208-sql-injection.html
- https://ccb.belgium.be/advisories/warning-litellm-pre-auth-sql-injection-cve-2026-42208-patch-immediately
- https://unaaldia.hispasec.com/2026/04/explotacion-rapida-de-una-inyeccion-sql-critica-en-litellm-pone-en-riesgo-claves-de-proveedores-de-llm.html

CVE-2026-3854 – GITHUB (EJECUCIÓN REMOTA DE CÓDIGO - RCE)

Se ha identificado una vulnerabilidad crítica de inyección de comandos en la infraestructura interna de procesamiento de Git de GitHub. El fallo permite a un usuario autenticado con acceso de escritura a un repositorio ejecutar código arbitrario en los servidores backend mediante una operación de git push especialmente diseñada.

Resumen técnico:

- Identificador principal: CVE-2026-3854.
- Severidad: 8.8 (Crítica) según el estándar de la industria.
- Causa raíz: Neutralización inadecuada de elementos especiales en las opciones de "git push" procesadas por el componente interno X-STAT.
- Mecanismo de falla: El sistema utilizaba el punto y coma (;) como delimitador en cabeceras internas de metadatos. Un atacante podía incluir este carácter en las opciones de push para inyectar campos adicionales, permitiendo manipular el entorno de ejecución (ej. rails_env), redirigir directorios de hooks y evadir protecciones de sandbox para ejecutar comandos como el usuario git.
- Estado de explotación: Reportado por investigadores de Wiz el 4 de marzo de 2026 a través del programa de Bug Bounty. GitHub corrigió el fallo en menos de dos horas y no se hallaron indicios de explotación maliciosa previa.
- Versiones afectadas: GitHub.com, GitHub Enterprise Cloud y GitHub Enterprise Server (GHES) en versiones anteriores a la 3.14.25, 3.15.20, 3.16.16, 3.17.13, 3.18.7, 3.19.4 y 3.20.0.

Impacto potencial:

- Ejecución remota de código (RCE): Control total sobre los nodos de almacenamiento de backend, permitiendo la ejecución de comandos con privilegios del servicio Git.
- Exposición multi-inquilino (Cross-tenant): En GitHub.com, la vulnerabilidad permitía potencialmente leer millones de repositorios privados pertenecientes a otras organizaciones alojados en el mismo nodo de almacenamiento.
- Compromiso total de instancias GHES: En entornos autogestionados (Enterprise Server), un atacante podría obtener acceso completo al sistema de archivos, configuraciones internas y secretos de la instancia.
- Evasión de políticas de seguridad: Capacidad para anular protecciones de sandbox y forzar la ejecución de scripts maliciosos incluso en entornos donde los hooks personalizados están deshabilitados.

Recomendaciones de mitigación:

1. Actualización inmediata de GitHub Enterprise Server: Migrar de forma urgente a las versiones parcheadas (3.14.25, 3.15.20, 3.16.16, 3.17.13, 3.18.7, 3.19.4, 3.20.0 o posteriores) para cerrar el vector de inyección.
2. Auditoría de registros de actividad: Revisar el archivo /var/log/github-audit.log en busca de operaciones de push que contengan el carácter ; en los valores de las opciones, lo cual podría indicar intentos de explotación.
3. Revisión de arquitecturas multi-servicio: Auditar cómo fluyen las entradas controladas por el usuario a través de protocolos internos compartidos, asegurando que los asunciones de seguridad de un servicio no sean vulneradas por otro.
4. Verificación para usuarios Cloud: No se requiere acción por parte de usuarios de GitHub.com o Enterprise Cloud, ya que la plataforma fue parcheada centralmente por el equipo de seguridad de GitHub.

Prioridad: Crítica.

Ampliar información:

- https://securityaffairs.com/191434/security/cve-2026-3854-github-flaw-enables-remote-code-execution.html
- https://www.csoonline.com/article/4164925/critical-github-rce-bug-exposed-millions-of-repositories.html
- https://github.blog/security/securing-the-git-push-pipeline-responding-to-a-critical-remote-code-execution-vulnerability/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-ejecucion-remota-de-codigo-en-github-enterprise-server-y-github-com/
- https://thehackernews.com/2026/04/researchers-discover-critical-github.html

CVE-2026-41940 – CPANEL & WHM (ACCESO NO AUTORIZADO)

Se ha identificado una vulnerabilidad crítica en los mecanismos de autenticación de las plataformas cPanel y WHM (WebHost Manager). El fallo permite a actores maliciosos eludir los procesos de inicio de sesión y obtener acceso administrativo a los paneles de control sin necesidad de credenciales válidas en ciertos escenarios.

Resumen técnico:

- Identificador principal: CVE-2026-41940
- ·Severidad: 9.3 (Crítica) según la escala CVSS v4.0.
- Causa raíz: Un fallo de seguridad que impacta directamente múltiples rutas de autenticación dentro del ecosistema principal del software.
- Mecanismo de falla: La vulnerabilidad afecta los procesos de login en los puertos TCP 2083 (cPanel) y 2087 (WHM), permitiendo que un atacante comprometa el acceso al servidor y tome control sobre cuentas y configuraciones.
- Estado de explotación: Reportada y corregida mediante parches de emergencia el 28 de abril de 2026; proveedores de hosting han aplicado bloqueos preventivos de puertos durante la mitigación.
- Versiones afectadas: Todas las versiones soportadas previas a las compilaciones seguras de abril de 2026 (específicamente versiones anteriores a la 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.136.0.5 y 11.134.0.20).

Impacto potencial:

- Control total del servidor (Nivel Root): Un atacante podría obtener privilegios administrativos completos en WHM, lo que le permite modificar protocolos de seguridad, gestionar certificados SSL y crear o eliminar cuentas de hosting.
- Exfiltración de datos sensibles: Acceso no autorizado a bases de datos corporativas, archivos de sitios web y comunicaciones por correo electrónico de todos los clientes alojados en el servidor afectado.
- Despliegue de Ransomware y Desfiguración: Capacidad para alterar masivamente el contenido de los sitios web (defacement) o cifrar información crítica para realizar extorsiones financieras.
- Uso de infraestructura para Botnets: Los servidores comprometidos pueden ser integrados en redes de bots para lanzar ataques de denegación de servicio (DDoS) o campañas masivas de spam malicioso.

Recomendaciones de mitigación:

1. Actualización inmediata a versiones parcheadas: Es imperativo actualizar los servidores a las versiones 11.110.0.97, 11.118.0.63, 11.126.0.54, 11.132.0.29, 11.134.0.20 o 11.136.0.5 mediante el comando /scripts/upcp --force.
2. Implementación de Autenticación Multifactor (MFA): Habilitar MFA de manera obligatoria para todas las cuentas administrativas para mitigar el riesgo de elusión de autenticación simple.
3. Restricción de acceso por dirección IP: Configurar reglas de firewall o listas blancas para permitir el acceso a las interfaces de administración (puertos 2083 y 2087) únicamente desde IPs corporativas confiables.
4. Auditoría de logs de autenticación: Revisar exhaustivamente los registros de acceso en busca de inicios de sesión inusuales o fallidos que pudieran haber ocurrido antes de la aplicación del parche.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/04/critical-cpanel-authentication.html
- https://blog.elhacker.net/2026/04/cpanel-advierte-sobre-fallo-critico-de.html#google_vignette
- https://ultimominuto.com.bo/ultimo-minuto/alerta-global-una-falla-critica-en-cpanel-whm-podria-comprometer-a-mas-de-40-millones-de-usuarios/
- https://blog.segu-info.com.ar/2026/04/vulnerabilidad-critica-de-autenticacion.html
- https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidad-critica-en-cpanel-whm/

MALWARE

RANSOMWARE KYBER – WINDOWS Y VMWARE ESXI (CIFRADO HÍBRIDO POST-CUÁNTICO)

Se ha detectado una nueva operación de ransomware denominada Kyber que está impactando simultáneamente entornos Windows y servidores VMware ESXi. La amenaza destaca por el uso coordinado de dos variantes que comparten infraestructura de mando y control (C2) basada en Tor para maximizar la interrupción operativa en infraestructuras críticas.

Resumen técnico:

- Tipo de amenaza: Ransomware multiplataforma (C++ para ESXi y Rust para Windows).
- Causa raíz: Explotación de servicios expuestos y movimiento lateral para alcanzar infraestructuras de virtualización y servidores de archivos.
- Mecanismo de cifrado (Windows): Implementa un esquema híbrido real que utiliza Kyber1024 (algoritmo resistente a computación cuántica) y X25519 para proteger las llaves simétricas, mientras que AES-256-CTR cifra los archivos.
- Mecanismo de cifrado (ESXi): Aunque la nota de rescate anuncia cifrado post-cuántico, el análisis técnico confirma el uso de ChaCha8 para archivos y RSA-4096 para llaves.
- Comportamiento en ESXi: Utiliza la utilidad nativa esxcli para enumerar y apagar máquinas virtuales (VM), cifra los datastores VMFS y desfigura las interfaces de gestión (MOTD y web) con la nota de rescate.
- Estado de la amenaza: Activa desde marzo de 2026; se ha confirmado el compromiso de contratistas de defensa y proveedores de servicios de TI.

Impacto potencial:

- Parálisis operativa total: La capacidad de atacar simultáneamente servidores de archivos Windows y el hipervisor ESXi permite un "apagón" operativo completo de la infraestructura empresarial.
- Eliminación de rutas de recuperación: La variante de Windows borra activamente Volume Shadow Copies (vssadmin), deshabilita la reparación de arranque y elimina registros de eventos para impedir la restauración local.
- Interrupción de servicios críticos: Detiene servicios de bases de datos (SQL Server), Exchange y soluciones de respaldo para liberar bloqueos de archivos y asegurar el cifrado total de la información.
- Inviabilidad de descifrado futuro: El uso de Kyber1024 en la versión de Windows asegura que las llaves permanezcan protegidas incluso ante el desarrollo de computación cuántica avanzada, eliminando la posibilidad de "cosechar ahora para descifrar después".

Recomendaciones de mitigación:

1. Fortalecimiento de hosts ESXi: Deshabilitar el acceso SSH en hipervisores donde no sea estrictamente necesario y aplicar autenticación multifactor (MFA) para todas las interfaces de gestión administrativa.
2. Protección de respaldos inmutables: Asegurar que las copias de seguridad se almacenen en repositorios fuera de línea o con políticas de inmutabilidad (WORM) para garantizar la recuperación sin pagar el rescate.
3. Restricción de herramientas administrativas: Limitar el uso de utilidades como vssadmin.exe, wmic.exe, wevtutil.exe y bcdedit.exe mediante políticas de control de ejecución (AppLocker o similares).
4. Monitoreo de indicadores de compromiso (IoC): Configurar alertas de seguridad para detectar la creación de archivos con las extensiones .#~~~ (Windows) y .xhsyw (ESXi), así como cambios anómalos en el archivo Message of the Day de VMware.

Prioridad: Urgente.

Ampliar información:

- https://www.pcrisk.com/internet-threat-news/35205-kyber-ransomware-and-the-post-quantum-illusion
- https://socprime.com/active-threats/kyber-ransomware-targets-windows-and-esxi/
- https://ciberblog.net/noticias/kyber-ransomware-post-quantum-windows-esxi
- https://blog.segu-info.com.ar/2026/04/ransomware-kyber-ataca-windows-y-esxi.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

COMPROMISO DE PAQUETES OFICIALES DE SAP EN EL REGISTRO NPM (MINI SHAI-HULUD)

Se ha detectado un ataque masivo a la cadena de suministro denominado "Mini Shai-Hulud", el cual comprometió cuatro paquetes oficiales del ecosistema SAP Cloud Application Programming Model (CAP). El ataque inyecta un sofisticado infostealer diseñado para exfiltrar credenciales de desarrolladores y secretos de entornos CI/CD.

Resumen técnico:

- Paquetes afectados: mbt@1.2.48, @cap-js/db-service@2.10.1, @cap-js/sqlite@2.2.2 y @cap-js/postgres@2.2.2.
- Vector de entrada: El atacante comprometió cuentas de mantenedores y abusó de configuraciones OIDC en flujos de GitHub Actions que carecían de puertas de aprobación manual.
- Mecanismo de infección: Los paquetes incluyen un gancho preinstall que ejecuta setup.mjs. Este cargador descarga el entorno de ejecución Bun desde GitHub para ejecutar un payload de 11.6 MB (execution.js) altamente ofuscado.
- Persistencia avanzada: El malware inyecta ganchos de ejecución en configuraciones de agentes de IA como Claude Code (.claude/settings.json) y tareas automáticas de VS Code (.vscode/tasks.json), reactivándose cada vez que el desarrollador abre el proyecto.
- Geofencing: El código incluye una lógica de salida temprana que aborta la ejecución si detecta un entorno con lenguaje o configuración regional de Rusia (ru).

Impacto potencial:

- Exfiltración masiva de secretos: Robo de tokens de GitHub/npm, llaves SSH, configuraciones de Kubernetes y credenciales maestras de proveedores de nube (AWS, Azure, GCP).
- Compromiso de la memoria del CI: En entornos de integración continua, el malware utiliza scripts de Python para leer la memoria del proceso del runner y extraer secretos en texto plano, evadiendo el enmascaramiento de logs.
- Propagación autónoma tipo gusano: El payload utiliza los tokens robados para inyectar código malicioso y publicar nuevas versiones en todos los repositorios y paquetes a los que el desarrollador tenga acceso.
- Secuestro de flujos de trabajo de IA: Al comprometer las configuraciones de agentes de codificación (Claude Code), el atacante garantiza la ejecución persistente de código malicioso durante el ciclo de vida del desarrollo.

Recomendaciones para mitigar el riesgo:

1. Rotación inmediata y conservadora de credenciales: Si se instaló una versión afectada, se deben revocar todos los tokens de npm, PATs de GitHub, llaves de nube y secretos de administradores de contraseñas (1Password, Bitwarden) accesibles desde la máquina comprometida.
2. Forzar la instalación sin scripts: Configurar los entornos de desarrollo y CI/CD para utilizar npm install --ignore-scripts por defecto, permitiendo ganchos de ciclo de vida únicamente para paquetes verificados manualmente.
3. Auditoría de persistencia en repositorios: Realizar una búsqueda exhaustiva en la organización de GitHub en busca de archivos .claude/settings.json o .vscode/tasks.json inusuales, así como ramas sospechosas con el nombre dependabout/.
4. Pinning a versiones seguras: Actualizar de forma inmediata a las versiones remediadas publicadas por SAP: @cap-js/db-service@2.11.0, @cap-js/sqlite@2.4.0, @cap-js/postgres@2.3.0 y mbt@1.2.49.

Prioridad: Importante.

Ampliar Información:

- https://www.bleepingcomputer.com/news/security/official-sap-npm-packages-compromised-to-steal-credentials/
- https://blog.segu-info.com.ar/2026/04/paquetes-oficiales-de-sap-npm.html
- https://thehackernews.com/2026/04/sap-npm-packages-compromised-by-mini.html
- https://www.cryptika.com/sap-npm-packages-compromised-to-harvest-developer-and-ci-cd-secrets/
- https://snyk.io/blog/bun-based-stealer-hits-sap-cap-js-mbt-npm-packages/