GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1326

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

VULNERABILIDADES

LANGCHAIN Y LANGGRAPH – EXPOSICIÓN DE ARCHIVOS, SECRETOS Y BASES DE DATOS (CVE-2026-34070, CVE-2025-68664, CVE-2025-67644)

Investigadores de seguridad han revelado tres vulnerabilidades críticas en los frameworks LangChain y LangGraph. Estos fallos permiten a atacantes externos acceder a datos sensibles de la empresa, incluyendo archivos del sistema, claves de API, variables de entorno e historiales de conversaciones, comprometiendo la base misma de las aplicaciones impulsadas por modelos de lenguaje (LLM).

Resumen técnico:

- Identificadores principales: CVE-2026-34070 (Salto de directorio), CVE-2025-68664 (Deserialización insegura), CVE-2025-67644 (Inyección SQL).
- Severidad: Hasta 9.3 (Crítica) según el fallo específico.
- Causa raíz: Validación deficiente de entradas en los componentes de carga de prompts, manejo de objetos serializados y filtros de metadatos.
- Mecanismo de falla: Los atacantes pueden suministrar plantillas de prompts maliciosas o estructuras de datos manipuladas que el framework interpreta como comandos u objetos legítimos, permitiendo la fuga de información del host.
- Estado de explotación: Parches publicados a finales de marzo de 2026; se advierte sobre un "efecto dominó" debido a la enorme cantidad de librerías que dependen de estos frameworks.
- Versiones afectadas: LangChain-Core (anteriores a 1.2.22 / 0.3.81) y LangGraph-checkpoint-sqlite (anteriores a 3.0.1).

Impacto potencial:

- Exfiltración de secretos de entorno: El fallo de deserialización permite extraer llaves de API y credenciales críticas almacenadas en las variables de entorno del servidor.
- Acceso arbitrario al sistema de archivos: Mediante el salto de directorio, un atacante puede leer archivos de configuración de Docker, archivos /etc/passwd o cualquier dato sensible del sistema operativo.
- Manipulación y robo de bases de datos: La inyección SQL en LangGraph permite ejecutar consultas arbitrarias contra la base de datos SQLite, exponiendo historiales completos de chats y estados de los agentes de IA.
- Compromiso de la cadena de suministro de IA: Debido a que cientos de librerías integran LangChain, una vulnerabilidad aquí afecta a todo el ecosistema derivado que hereda el código vulnerable.

Recomendaciones de mitigación:

1. Actualización inmediata de dependencias: Migrar urgentemente a langchain-core >= 1.2.22 (o versiones específicas 0.3.81 / 1.2.5) y langgraph-checkpoint-sqlite >= 3.0.1.
2. Auditoría de carga de configuraciones: Revisar cualquier código que pase configuraciones externas a funciones como load_prompt_from_config() para asegurar que no provengan de fuentes no confiables.
3. Deshabilitar secretos en la deserialización: Asegurarse de mantener el nuevo valor por defecto secrets_from_env=False al deserializar datos para evitar la fuga automática de variables de entorno.
4. Validación estricta de metadatos: Nunca permitir que cadenas controladas por el usuario se conviertan directamente en claves de diccionario para operaciones de filtrado en bases de datos.

Prioridad: Crítica.

Ampliar información:

- https://www.csoonline.com/article/4151814/langchain-path-traversal-bug-adds-to-input-validation-woes-in-ai-pipelines.html
- https://www.prosec-networks.com/en/blog/ki-sicherheitsrisiko-langchain-langgraph-schwachstellen/
- https://www.techradar.com/pro/security/each-vulnerability-exposes-a-different-class-of-enterprise-data-langchain-framework-hit-by-several-worrying-security-issues-heres-what-we-know
- https://thehackernews.com/2026/03/langchain-langgraph-flaws-expose-files.html

GOOGLE CLOUD VERTEX AI – ABUSO DE AGENTES Y ESCALADA DE PRIVILEGIOS

Investigadores de Unit 42 han revelado una vulnerabilidad crítica en la plataforma Vertex AI de Google Cloud que permite convertir agentes de IA en "dobles agentes". Debido a una configuración excesiva de permisos por defecto en las cuentas de servicio administradas por Google (P4SA), un atacante puede extraer credenciales para acceder a datos sensibles de clientes y a la infraestructura interna de Google, incluyendo repositorios de código privado.

Resumen técnico:

- Identificador principal: Riesgo de configuración en el Agent Development Kit (ADK) de Vertex AI.
- Severidad: Crítica (Impacto de escalada de privilegios y exfiltración de datos).
- Causa raíz: Asignación excesiva de permisos por defecto en el Per-Project, Per-Product Service Agent (P4SA).
- Mecanismo de falla: Al desplegar un agente, las llamadas al servicio de metadatos de Google exponen tokens de acceso que permiten a un atacante salir del contexto de ejecución del agente hacia el proyecto del consumidor.
- Estado de explotación: Documentado por investigadores en marzo de 2026; Google ha actualizado su documentación y recomendado cambios en la arquitectura de permisos.
- Versiones afectadas: Despliegues de Vertex AI Agent Engine que utilicen las cuentas de servicio predeterminadas de Google.

Impacto potencial:

- Acceso no autorizado a Cloud Storage: El atacante puede obtener lectura irrestricta de todos los buckets de almacenamiento dentro del proyecto de Google Cloud de la organización.
- Exposición de propiedad intelectual de Google: Se confirmó que las credenciales robadas permitieron descargar imágenes de contenedores privados del Artifact Registry de Google, revelando planos de su infraestructura interna.
- Riesgo de ejecución remota de código (RCE): El uso de archivos code.pkl (Python Pickle) para serializar agentes facilita backdoors persistentes mediante la ejecución de código arbitrario durante la deserialización.
- Amenaza interna automatizada: Un agente comprometido puede actuar de forma autónoma para mapear la cadena de suministro de software interna y planificar ataques laterales de gran escala.

Recomendaciones de mitigación:

1. Implementación de BYOSA (Bring Your Own Service Account): Reemplazar el agente de servicio por defecto por una cuenta de servicio dedicada y personalizada para aplicar el principio de menor privilegio (PoLP).
2. Restricción de Scopes de OAuth: Revisar y limitar los alcances de OAuth 2.0 asignados, evitando que los agentes tengan acceso innecesario a servicios de Google Workspace (Gmail, Drive).
3. Validación de integridad de fuentes: Tratar el despliegue de agentes de IA con el mismo rigor que el código de producción, validando límites de permisos antes del despliegue en entornos críticos.
4. Monitoreo de identidades (CIEM): Utilizar herramientas de gestión de derechos de infraestructura en la nube para detectar anomalías en el uso de tokens y accesos cruzados entre proyectos.

Prioridad: Crítica.

Ampliar información:

- https://www.somo.nl/big-tech-sets-unfair-terms-and-conditions-for-ai-data-workers-globally/
- https://dev.to/waxell/your-agent-monitoring-sdk-was-the-backdoor-ed9
- https://www.darkreading.com/cyber-risk/googles-vertex-ai-over-privilege-problem
- https://unit42.paloaltonetworks.com/double-agents-vertex-ai/
- https://thehackernews.com/2026/03/vertex-ai-vulnerability-exposes-google.html

TRUECONF – EJECUCIÓN ARBITRARIA MEDIANTE ABUSO DE ACTUALIZACIÓN (CVE-2026-3502)

Se ha detectado una vulnerabilidad Zero-Day de alta severidad en el cliente de videoconferencia TrueConf, utilizada en la campaña de ciberespionaje denominada "TrueChaos". El fallo permite a un atacante que haya comprometido el servidor local (on-premises) distribuir actualizaciones maliciosas a todos los usuarios conectados, ejecutando código arbitrario en los endpoints sin necesidad de interacción adicional o phishing.

Resumen técnico:

- Identificador principal: CVE-2026-3502.
- Severidad: 7.8 (Alta) en la escala CVSS v3.1.
- Causa raíz: Falta de verificación de integridad y autenticidad en el mecanismo de descarga de actualizaciones del cliente.
- Mecanismo de falla: El cliente confía ciegamente en el servidor local para obtener nuevas versiones. Un atacante sustituye el instalador legítimo por uno "envenenado" que utiliza técnicas de DLL Side-loading para desplegar backdoors.
- Estado de explotación: Explotado activamente a inicios de 2026 contra redes gubernamentales en el sudeste asiático por actores vinculados a China.
- Versiones afectadas: Clientes de TrueConf para Windows anteriores a la versión 8.5.3.

Impacto potencial:

- Compromiso masivo de endpoints: Un solo servidor comprometido permite infectar de forma simultánea a todos los empleados o entidades que dependan de esa infraestructura de comunicación.
- Despliegue de frameworks de Post-Explotación: Se ha confirmado el uso de esta vulnerabilidad para instalar el framework Havoc, permitiendo control total sobre las máquinas afectadas.
- Escalada de privilegios y persistencia: El malware utiliza el secuestro de orden de carga de DLL (como iscsiexe.dll) para evadir el Control de Cuentas de Usuario (UAC) y mantenerse en el sistema tras reinicios.
- Espionaje gubernamental y militar: Dado que TrueConf se utiliza en entornos aislados (air-gapped) o de alta seguridad, el impacto directo es el robo de información estratégica y confidencial.

Recomendaciones de mitigación:

1. Actualización urgente del cliente: Migrar de forma inmediata a TrueConf para Windows v8.5.3 o superior, que incorpora firmas criptográficas y validación de integridad en las actualizaciones.
2. Monitoreo de procesos sospechosos: Vigilar la aparición de ejecutables no firmados o inusuales en rutas como C:\ProgramData\PowerISO\ o %AppData%\Roaming\Adobe\.
3. Auditoría del servidor TrueConf: Reforzar la seguridad del servidor central (on-premises), ya que su compromiso es el requisito previo para el éxito de este ataque de cadena de suministro interna.
4. Búsqueda de IoCs (Hunting): Rastrear la creación de archivos como 7z-x64.dll o comunicaciones hacia IPs de C2 identificadas (ej. 47.237.15.197) relacionadas con la infraestructura de Havoc.

Prioridad: Urgente.

Ampliar información:

- https://blog.checkpoint.com/research/when-trusted-software-updates-become-the-attack-vector-inside-operation-truechaos-and-a-new-zero-day-vulnerability-in-a-popular-collaboration-tool/
- https://securityonline.info/trueconf-zero-day-vulnerability-cve-2026-3502-truechaos-campaign/
- https://research.checkpoint.com/2026/operation-truechaos-0-day-exploitation-against-southeast-asian-government-targets/
- https://thehackernews.com/2026/03/trueconf-zero-day-exploited-in-attacks.html

MALWARE

DEEPLOAD: LOADER CON EVASIÓN ASISTIDA POR IA Y PERSISTENCIA MEDIANTE WMI

Investigadores de ReliaQuest han identificado una nueva campaña de malware denominada DeepLoad, diseñada para el robo de credenciales en entornos empresariales. Lo que distingue a esta amenaza es su sofisticada cadena de ataque que utiliza ingeniería social tipo ClickFix combinada con capas de ofuscación generadas presumiblemente por Inteligencia Artificial, permitiéndole evadir soluciones de escaneo estático tradicionales.

Resumen técnico:

- Vector de ataque: Técnica ClickFix, que engaña al usuario para que ejecute comandos de PowerShell directamente en su terminal bajo la falsa premisa de solucionar errores del sistema.
- Evasión avanzada: Utiliza una capa de ofuscación masiva con miles de asignaciones de variables sin sentido (ruido) para confundir el análisis estático. Se oculta inyectando su carga útil en el proceso legítimo de Windows LockAppHost.exe (pantalla de bloqueo).
- Capacidad de propagación: El malware tiene la capacidad de detectar unidades USB conectadas y copiar archivos maliciosos con nombres de instaladores comunes (ej. ChromeSetup.lnk), facilitando el movimiento lateral.
- Persistencia sigilosa: Implementa suscripciones a eventos de Windows Management Instrumentation (WMI), lo que permite que el sistema se reinfecte automáticamente días después de una limpieza estándar si no se eliminan estos registros específicos.

Impacto potencial:

- Robo de credenciales en tiempo real: A diferencia de otros stealers, DeepLoad incluye un registrador de pulsaciones (keylogger) y una extensión de navegador maliciosa que captura contraseñas y tokens de sesión mientras el usuario los escribe.
- Reinfección persistente: La capacidad de ocultarse en WMI rompe las cadenas de procesos tradicionales, permitiendo que el ataque se ejecute nuevamente tras reinicios o limpiezas superficiales de archivos.
- Compromiso de dispositivos extraíbles: La infección automática de memorias USB convierte a cualquier dispositivo conectado en un vector de propagación para el resto de la red corporativa.
- Acceso administrativo y exfiltración: El uso de herramientas como filemanager.exe (disfrazado de utilidad del sistema) garantiza una vía de escape para los datos robados incluso si el cargador principal es detectado.

Recomendaciones de mitigación:

1. Habilitar PowerShell Script Block Logging: Es la única forma confiable de registrar y analizar los comandos reales que PowerShell ejecuta en tiempo de ejecución, eliminando el ruido de la ofuscación por IA.
2. Auditoría de suscripciones WMI: Realizar una búsqueda proactiva de suscripciones a eventos de WMI en los hosts afectados para eliminar mecanismos de persistencia que los antivirus estándar podrían omitir.
3. Rotación obligatoria de credenciales: Si se confirma una infección, es imperativo rotar todas las contraseñas y tokens de sesión utilizados durante el periodo de compromiso, ya que el malware captura datos en vivo.
4. Monitoreo de procesos críticos: Configurar alertas de EDR para detectar conexiones de red inusuales desde procesos como LockAppHost.exe, makecab.exe o Magnify.exe, que normalmente no deberían iniciar tráfico externo.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/03/deepload-malware-uses-clickfix-and-wmi.html
- https://ciberconcienciadigital.com/noticia.php?id=503
- https://www.infosecurity-magazine.com/news/deepload-malware-clickfix-ai-code/
- https://reliaquest.com/blog/threat-spotlight-deepload-malware-pairs-clickfix-delivery-with-ai-generated-evasion/
- https://www.scworld.com/brief/ai-powers-clandestine-deepload-credential-stealing-campaign

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

EXPLOTACIÓN ACTIVA DE SQLi CRÍTICA EN FORTINET FORTICLIENT EMS (CVE-2026-21643)

Empresas de inteligencia de amenazas han detectado una campaña de explotación activa contra servidores FortiClient EMS (Endpoint Management Server). La vulnerabilidad permite a atacantes remotos no autenticados ejecutar código arbitrario mediante inyecciones SQL enviadas a través de cabeceras HTTP manipuladas, comprometiendo la gestión centralizada de toda la flota de dispositivos de la organización.

Resumen técnico:

- Identificador principal: CVE-2026-21643.
- Severidad: 9.8 (Crítica) en la escala CVSS v3.1.
- Causa raíz: Neutralización incorrecta de elementos especiales en comandos SQL (CWE-89) dentro de la capa de conexión a la base de datos.
- Mecanismo de falla: El atacante aprovecha el endpoint público /api/v1/init_consts enviando sentencias SQL maliciosas en la cabecera HTTP Site. Al no haber sanitización previa a la autenticación, el servidor ejecuta los comandos directamente contra la base de datos PostgreSQL.
- Estado de explotación: Confirmada por firmas como Defused y Shadowserver desde el 24 de marzo de 2026. Existen pruebas de concepto (PoC) públicas y se estiman más de 2,000 instancias expuestas globalmente.
- Versiones afectadas: Específicamente la versión 7.4.4 de FortiClient EMS.

Impacto potencial:

- Ejecución remota de código (RCE): El atacante puede tomar control total del servidor de administración, permitiendo la entrega de malware a todos los endpoints gestionados.
- Extracción de datos sensibles: Acceso irrestricto al inventario de dispositivos, políticas de seguridad corporativas, certificados de endpoints y credenciales de administrador.
- Compromiso multi-inquilino: En implementaciones multi-tenant, un atacante puede saltar entre diferentes sitios de clientes, exponiendo la información de múltiples organizaciones desde una sola instancia.
- Punto de entrada para ransomware: El control del EMS facilita el movimiento lateral profundo y la desactivación de protecciones en los endpoints antes de un despliegue de ransomware.

Recomendaciones para mitigar el riesgo:

1. Actualización inmediata a v7.4.5: Fortinet liberó el parche correctivo en febrero; es crítico migrar a la versión 7.4.5 o superior de inmediato si se utiliza la rama 7.4.
2. Restricción de acceso a la interfaz: Las consolas de administración EMS nunca deben estar expuestas directamente a internet. Se debe restringir el acceso únicamente vía VPN o mediante listas de control de acceso (ACLs) estrictas.
3. Monitoreo de cabeceras HTTP: Revisar logs del WAF o del servidor web en busca de inyecciones SQL en la cabecera Site, especialmente dirigidas al endpoint /api/v1/init_consts.
4. Aislamiento e investigación: Si el servidor estuvo expuesto sin el parche durante la última semana de marzo, debe tratarse como potencialmente comprometido y someterse a una revisión forense completa.

Prioridad: Urgente.

Ampliar Información:

- https://blog.segu-info.com.ar/2026/03/otra-vulnerabilidad-sqli-esta-siendo.html
- https://www.securityweek.com/exploitation-of-critical-fortinet-forticlient-ems-flaw-begins/
- https://ciberblog.net/noticias/forticlient-ems-sql-injection-ataque-activo
- https://nksistemas.com/alerta-de-seguridad-vulnerabilidad-sqli-critica-en-fortinet-forticlient-ems-cve-2026-21643/
- https://www.helpnetsecurity.com/2026/03/30/forticlient-ems-cve-2026-21643-reported-exploitation/