GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición °3126

## 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 | 1 | 0 |

## VULNERABILIDADES

### AZURE COSMOS DB – ESCAPE DE SANDBOX Y ACCESO ENTRE TENANTS (COSMOSESCAPE)

Se ha divulgado la identificación de una cadena de vulnerabilidades críticas en la API Gremlin de Azure Cosmos DB, denominada CosmosEscape, que permitía a un atacante remoto no autenticado o con una cuenta básica del servicio evadir el entorno aislado (sandbox) del motor de consultas, lograr ejecución remota de código en la infraestructura compartida y extraer una clave de firma global (Cosmos Master Key) capaz de acceder con privilegios totales de lectura y escritura a cualquier base de datos alojada en la plataforma.

**Resumen técnico:**

- Identificador principal: Sin CVE asignado (Denominación clave: CosmosEscape).
- Severidad: Crítica (Severidad máxima a nivel de plano de gestión / Impacto de control total sin requerir privilegios previos).
- Causa raíz: Inadecuada restricción de reflexión en .NET (CWE-470) dentro del motor personalizado de compilación y ejecución de consultas Gremlin.
- Mecanismo de falla: El motor de Cosmos DB traduce las consultas Gremlin a código .NET y las ejecuta en un entorno restringido. La falta de controles sobre la capacidad de reflexión (reflection) de .NET permitió a los investigadores evadir el sandbox, construir primitivas de lectura/escritura de archivos y obtener ejecución arbitraria de código en el componente DB Gateway (ejecutado sobre clústeres multiinquilino de Azure Service Fabric). A través de credenciales del clúster, se accedió a la Cosmos Master Key y al Config Store (directorio regional de cuentas), permitiendo consultar cualquier ID de inquilino/suscripción y extraer la clave primaria (Primary Key) de cualquier cuenta de Cosmos DB en la plataforma.
- Estado de explotación: Divulgada públicamente el 30 de julio de 2026 por Wiz Research (con apoyo de su sistema autónomo de investigación de vulnerabilidades con IA, Atlas). No existen evidencias de explotación no autorizada en entornos reales. Microsoft aplicó un parche inicial dentro de las 48 horas tras la notificación en noviembre de 2025 y completó la solución arquitectónica global (eliminando la Cosmos Master Key) en julio de 2026.
- Versiones afectadas: Todas las cuentas e interfaces de Azure Cosmos DB (SQL, MongoDB, Cassandra y Gremlin), incluyendo bases de datos de servicios internos de Microsoft (Entra ID, Teams, Copilot) y despliegues con aislamiento de red o Private Endpoints.

**Impacto potencial:**

- Toma de control total y manipulación arbitraria de datos: La extracción de las claves primarias (Primary Keys) otorga acceso irrestricto de lectura, escritura y eliminación sobre cualquier base de datos, contenedor o documento alojado en la cuenta comprometida.
- Reconocimiento y focalización estratégica de objetivos corporativos: El acceso al Config Store permitía a un atacante listar e inspeccionar todas las cuentas de una región y filtrarlas por ID de inquilino (Tenant ID) o ID de suscripción de Azure para ubicar con precisión las bases de datos de organizaciones específicas.
- Bypass completo de aislamientos perimetrales y redes privadas: Dado que el componente DB Gateway comprometido es el encargado de validar y aplicar los límites de red, la explotación permitía acceder a cuentas con restricciones de firewall, aisladas de Internet o configuradas con Private Endpoints.
- Riesgo de compromiso transversal en servicios centrales de Microsoft: Debido a que Cosmos DB respalda servicios como Microsoft Entra ID, Teams y Copilot, la vulnerabilidad exponía teóricamente datos de autenticación, historiales de conversación y registros operativos de la infraestructura interna de Microsoft.

**Recomendaciones de mitigación:**

1. Verificación de la remediación arquitectónica en la plataforma: Confirmar que el entorno opere sobre la plataforma actualizada por el fabricante en julio de 2026, la cual eliminó definitivamente la credencial Cosmos Master Key y reforzó la autenticación servicio a servicio.
2. Auditoría defensiva y cacería de amenazas en logs de auditoría: Revisar los registros de acceso e historial de auditoría de Cosmos DB previos a noviembre de 2025 en busca de solicitudes anómalas de claves primarias, enumeración de bases de datos o conexiones originadas en direcciones IP no reconocidas.
3. Adopción de identidades administradas y control de acceso basado en roles (RBAC): Reducir o eliminar el uso de claves primarias estáticas compartidas, migrando hacia Azure Managed Identities y políticas RBAC granulares para restringir el alcance de eventuales compromisos de credenciales.
4. Implementación de cifrado del lado del cliente (Client-Side Encryption): Aplicar mecanismos de cifrado de datos antes de transmitirlos a la base de datos administrada, garantizando que la información confidencial permanezca protegida incluso ante hipotéticas vulnerabilidades en el plano de gestión del proveedor de nube.

**Prioridad: Crítica.**

**Ampliar información:**

- https://www.wiz.io/blog/cosmosescape-taking-over-every-database-in-azure-cosmos-db
- https://thehackernews.com/2026/07/azure-cosmos-db-flaw-exposed-platform.html
- https://www.diariobitcoin.com/tecnologia/una-falla-critica-pudo-comprometer-todas-las-bases-de-datos-de-azure-cosmos-db/
- https://www.csoonline.com/article/4204925/critical-azure-cosmos-db-flaw-threatened-cross-tenant-database-takeover.html
- https://www.techtimes.com/articles/322337/20260730/cosmosescape-wiz-research-breached-azure-cosmos-db-gateway-extracted-key-every-database.htm

## ADOBE CAMPAIGN CLASSIC – EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-48449)

Adobe ha publicado un aviso de seguridad para corregir una vulnerabilidad de severidad máxima (CVSS 10.0) en Adobe Campaign Classic (ACC), su plataforma empresarial de automatización de marketing. El fallo se debe a una falla de autorización que permite a un atacante remoto no autenticado ejecutar código arbitrario a través de la red en el contexto de la cuenta de usuario del servicio, sin requerir ningún tipo de interacción de un usuario legítimo.

**Resumen técnico:**

- Identificador principal: CVE-2026-48449 (Boletín de seguridad de Adobe: APSB26-114).
- Severidad: Crítica (CVSS v3.1: 10.0 / Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).
- Causa raíz: Autorización incorrecta (CWE-863) en la evaluación de solicitudes hacia operaciones privilegiadas.
- Mecanismo de falla: El software no valida ni aplica de forma estricta las restricciones de acceso del lado del servidor en sus puntos de enlace (endpoints). Un atacante remoto puede enviar peticiones maliciosas especialmente diseñadas para omitir los controles de autorización e invocar funciones restringidas. Debido a que el vector califica con cambio de alcance (S:C), la ejecución remota de código en el contexto del usuario de ACC excede los límites del componente afectado, pudiendo comprometer datos e infraestructura adyacente conectada a la plataforma. En el mismo boletín se abordó la falla de inyección SQL CVE-2026-48448 (CVSS 8.6), que permite la lectura arbitraria de archivos del sistema.
- Estado de explotación: Divulgada oficialmente por Adobe el 29/30 de julio de 2026. Aunque el fabricante indicó no registrar evidencia de ataques en curso al momento de la publicación, la ausencia de requisitos de autenticación e interacción la convierte en un objetivo de alta prioridad para escaneo y explotación masiva.
- Versiones afectadas: Adobe Campaign Classic (ACC v7) versiones 7.4.3 build 9397 y anteriores en plataformas Windows y Linux (afecta a implementaciones On-Premise e híbridas; las instancias en la nube gestionadas por Adobe fueron corregidas por el proveedor).

**Impacto potencial:**

- Ejecución remota de código sin interacción (Zero-Click): Permite a atacantes remotos no autenticados tomar el control técnico de los servidores de procesamiento sin requerir ninguna acción previa por parte de administradores o usuarios.
- Compromiso masivo de datos confidenciales (PII): Acceso irrestricto de lectura y modificación a las bases de datos de clientes, listas de suscriptores, credenciales de integración de red y registros de campañas masivas de marketing.
- Propagación lateral y cambio de alcance de seguridad: Al alterarse la autoridad de seguridad (Scope Change), la ejecución de código faculta la interacción con bases de datos backend corporativas, repositorios de archivos del sistema operativo y APIs de terceros integradas a ACC.
- Interrupción de operaciones y riesgo de persistencia: Capacidad para alterar o suspender el envío de comunicaciones corporativas, inyectar contenido malicioso en campañas dirigidas a clientes o desplegar herramientas de persistencia (web shells, tareas programadas) en el servidor.

**Recomendaciones de mitigación:**

1. Actualización inmediata de la plataforma On-Premise: Actualizar de manera prioritaria todas las instancias de Adobe Campaign Classic v7 a la versión 7.4.3 build 9398 o superior en entornos Windows y Linux.
2. Aislamiento perimetral y restricción de red: Bloquear la exposición directa de las interfaces de administración y APIs de ACC a la Internet pública, permitiendo el acceso únicamente a través de redes privadas virtuales (VPN), ZTNA o subredes de gestión autorizadas.
3. Endurecimiento de privilegios en el sistema operativo: Aplicar el principio de menor privilegio al usuario de servicio que ejecuta la aplicación ACC, restringiendo su capacidad de escribir en directorios críticos del sistema y ejecutar intérpretes de comandos (cmd.exe, powershell, bash).
4. Monitoreo defensivo e inspección de logs: Configurar reglas de detección en el Web Application Firewall (WAF) para bloquear peticiones no autenticadas hacia endpoints privilegiados, monitoreando la creación de procesos hijo inusuales o llamadas a comandos externos (curl, wget) desde el servicio de ACC.

**Prioridad: Crítica.**

**Ampliar información:**

- https://helpx.adobe.com/ar/security/products/campaign/apsb26-114.html
- https://ciberconcienciadigital.com/noticia.php?id=961
- https://www.sentinelone.com/vulnerability-database/cve-2026-48449/
- https://thehackernews.com/2026/08/adobe-campaign-classic-cvss-100-flaw.html
- https://cyberworldops.eu/es/adobe-corrige-una-vulnerabilidad-critica-en-campaign-classic-cvss-100
- https://securityaffairs.com/196429/security/adobe-fixed-a-maximum-severity-vulnerability-flaw-in-campaign-classic.html

## CPANEL & WHM – ESCALADA DE PRIVILEGIOS MEDIANTE SQL ROOT (CVE-2026-58048)

Se ha divulgado una vulnerabilidad crítica de escalada de privilegios en la funcionalidad de gestión de bases de datos de cPanel & WHM y WP Squared, la cual permite a cualquier cliente de alojamiento web autenticado con acceso estándar al módulo de MySQL/MariaDB ejecutar comandos SQL arbitrarios en el contexto del usuario administrador (root) de la base de datos. Esta falla rompe el límite de aislamiento entre inquilinos en entornos de hosting compartido y, dependiendo de la configuración del sistema operativo y del motor de base de datos, puede escalar hasta el compromiso total del servidor.

**Resumen técnico:**

- Identificador principal: CVE-2026-58048.
- Severidad: Crítica (CVSS v4.0: 9.4 / Severidad máxima a nivel de base de datos multiinquilino).
- Causa raíz: Falla en la preservación del modo SQL (SQL mode) durante el flujo de trabajo de renombrado de bases de datos (Clasificado bajo CWE-89 / Inyección SQL y elevación de privilegios).
- Mecanismo de falla: Durante el renombrado de una base de datos**,** cPanel crea una base temporal, migra los datos, recrea permisos y código almacenado y elimina la original. En este proceso no conserva correctamente el modo SQL**,** lo que permite que las sentencias se ejecuten con privilegios de root de MySQL/MariaDB en lugar de los permisos restringidos de la cuenta de cPanel**.**
- Estado de explotación: Divulgada oficialmente a principios de agosto de 2026 por cPanel/WebPros tras el reporte responsable del investigador Vincent55 Yang. CISA registró la falla reconociendo su impacto total pero evaluándola inicialmente como de baja automatización. No obstante, al afectar a cualquier cliente autenticado, representa un riesgo inminente en servidores compartidos.
- Versiones afectadas: Todas las versiones soportadas de cPanel & WHM y WP Squared no parcheadas. Las versiones corregidas corresponden a las compilaciones 11.110.0.137, 11.118.0.71, 11.126.0.78, 11.134.0.48, 11.136.0.32 y 138.1.6 (para WP Squared).

**Impacto potencial:**

- Escalada de privilegios a nivel administrativo de base de datos: Un usuario con permisos limitados de hosting puede ejecutar cualquier instrucción SQL con derechos de SUPER/root, sobrepasando las restricciones impuestas por la plataforma.
- Compromiso transversal de datos entre clientes (Cross-Tenant Data Exposure): En entornos de hosting compartido, el atacante puede listar, exfiltrar, alterar o borrar las bases de datos de otros clientes alojados en el mismo servidor físico o virtual.
- Potencial compromiso del Sistema Operativo subyacente: Si los motores MySQL o MariaDB operan con permisos elevados sobre el sistema de archivos (o con opciones como INTO OUTFILE / LOAD DATA INFILE habilitadas), la vulnerabilidad permite la lectura/escritura de archivos locales del servidor y la ejecución remota de comandos a nivel de SO.
- Persistencia maliciosa e inyección de código: Capacidad para alterar usuarios administradores del motor de BD, modificar procedimientos almacenados, crear triggers maliciosos o comprometer claves y credenciales de aplicaciones web hospedadas (como plataformas WordPress o cPanel Team Users).

**Recomendaciones de mitigación:**

1. Actualización prioritaria a versiones parcheadas: Aplicar de inmediato la actualización de cPanel & WHM mediante la consola de WHM o ejecutando la actualización forzada desde la línea de comandos (/usr/local/cpanel/scripts/upcp --force).
2. Mitigación temporal vía Feature Manager (si no es posible parchear de inmediato): Revocar la característica/módulo "MySQL" dentro de las listas de funciones (Feature Lists) asignadas a los usuarios de cPanel. Esto no afecta el funcionamiento de las bases de datos en producción existentes, pero bloquea la adición, eliminación o renombrado de bases de datos.
3. Auditoría e inspección defensiva en registros de MySQL/MariaDB: Inspeccionar los logs de auditoría de la base de datos en busca de consultas sospechosas ejecutadas por cuentas root, creación inusual de usuarios, asignaciones anómalas de privilegios o llamadas a archivos del sistema.
4. Endurecimiento de privilegios del motor de base de datos: Verificar que el servicio de base de datos opere bajo un usuario con privilegios mínimos en el sistema operativo (chroot o permisos de archivo restringidos) para evitar que una escalada en la BD comprometa el kernel o el sistema operativo.

**Prioridad: Crítica.**

**Ampliar información:**

- https://blog.segu-info.com.ar/2026/08/vulnerabilidad-critica-en-cpanel.html
- https://thehackernews.com/2026/08/new-cpanel-critical-flaw-could-let.html
- https://devel.group/blog/vulnerabilidad-critica-de-escalada-de-privilegios-en-cpanel-y-whm-cve-2026-58048/
- https://support.cpanel.net/hc/en-us/articles/42285745783703-Security-CVE-2026-58048-Database-Privilege-Escalation
- https://blog.elhacker.net/2026/08/vulnerabilidad-critica-de-cpanel.html
- https://www.itwaarschuwing.nl/es/vulnerabilidad-critica-cpanel-sql-privilegios/
- https://securityaffairs.com/196595/security/cve-2026-58048-cpanel-bug-enables-full-database-administrator-access.html

## MALWARE

### CLICKFIX + ATOMIC STEALER (AMOS) PARA MACOS (INFRAESTRUCTURA DE EVASIÓN VÍA BROWSER FINGERPRINTING)

Microsoft Threat Intelligence ha identificado una amplia infraestructura maliciosa compuesta por más de 250 dominios que utilizan tácticas de ingeniería social tipo ClickFix para distribuir la amenaza Atomic Stealer (AMOS) y MacSync en sistemas macOS. La operación destaca por incorporar un mecanismo de control del lado del servidor (browser fingerprinting) diseñado para inspeccionar los navegadores de las víctimas y evadir entornos de análisis (sandboxes) antes de entregar los comandos de infección.

**Resumen técnico:**

- Identificador principal: Campaña ClickFix / Atomic Stealer (AMOS) & MacSync para macOS.
- Tipo de amenaza: Infostealer para macOS, cargador malicioso (loader) e ingeniería social avanzada.
- Mecanismo de acceso e infección: La campaña utiliza sitios web clonados (como portales falsos de GitHub o interfaces de inicio de sesión) que muestran errores simulados o verificaciones CAPTCHA. Mediante engaños (ClickFix), la página copia automáticamente un comando cifrado al portapapeles del usuario y lo induce a abrir la Terminal de macOS y pegarlo (Ctrl + V / Cmd + V + Enter), ejecutando un script remoto vía curl canalizado a zsh.
- Mecanismos de evasión y fingerprinting: Antes de mostrar la trampa, un script ejecutable en JavaScript (~2.5 KB) analiza variables del navegador para confirmar que la visita proviene de un hardware Apple real. Valida la cadena de plataforma (MacIntel), dimensiones de pantalla, renderizado WebGL, zona horaria y ausencia de herramientas de análisis o consolas de desarrollador abiertas. Si detecta un entorno virtual o crawler, muestra una página en blanco o benigna; si califica como un equipo Mac real, despliega el falso portal de descarga.
- Capacidades del malware (AMOS): Una vez ejecutado el script, se despliega el troyano infostealer AMOS, el cual extrae credenciales e historiales guardados en navegadores, claves de acceso al Keychain de macOS, frases semilla y llaves de billeteras de criptomonedas, datos de sesión y archivos confidenciales del usuario, exfiltrándolos mediante peticiones HTTP POST salientes.
- Estado de actividad: Operación activa y en evolución detectada por Microsoft a principios de agosto de 2026.

**Impacto potencial:**

- Compromiso masivo de credenciales e identidades corporativas: Exfiltración directa de contraseñas guardadas en navegadores (Chrome, Safari, Brave, Edge), tokens de sesión activos de aplicaciones SaaS y secretos almacenados en el Keychain nativo del sistema.
- Substracción de activos digitales y billeteras de criptomonedas: Robo de frases de recuperación (seed phrases) y claves privadas asociadas a extensiones y aplicaciones locales de criptoactivos.
- Evasión efectiva de defensas tradicionales y sandboxes de red: El filtrado previo mediante browser fingerprinting impide que rastreadores automatizados y entornos de detonación detecten el código malicioso, pasando desapercibido ante listas de reputación.
- Ejecución directa impulsada por el usuario (Bypass de perímetro): Al lograr que la propia víctima ejecute el comando en la Terminal con permisos del usuario activo, el ataque elude la necesidad de descargar e instalar binarios tradicionales o archivos de imagen de disco (.dmg).

**Recomendaciones de mitigación:**

1. Concientización y entrenamiento ante la regla de oro de ClickFix: Capacitar a los usuarios bajo el principio de que ningún sitio web, CAPTCHA o soporte técnico legítimo solicitará jamás copiar y ejecutar comandos directamente en la Terminal o consola del sistema operativo.
2. Monitoreo e inspección de procesos en la Terminal de macOS: Implementar reglas en soluciones EDR para auditar la ejecución de la consola (Terminal.app) cuando inicie comandos que combinen curl o wget canalizados hacia intérpretes de comandos (zsh, bash) o invocaciones a osascript.
3. Aprovechamiento de las protecciones nativas de macOS y parches: Mantener las estaciones de trabajo actualizadas a macOS 26.4 o superior (las cuales incluyen alertas de confirmación al pegar comandos en la Terminal) y asegurar la actualización constante del motor antivirus integrado Apple XProtect.
4. Detección de artefactos de fingerprinting e infraestructura: Configurar firmas defensivas en soluciones de seguridad web y SIEM para identificar formularios de recolección de métricas (artefactos como mode:"php") y bloquear tráfico saliente hacia endpoints de descarga del tipo /curl/<id>.

**Prioridad: Urgente.**

**Ampliar información:**

- https://www.xataka.com.mx/seguridad/cuidate-falsos-captcha-mexico-asi-funciona-clickfix-engano-que-puede-hackear-tu-computadora
- https://spotontech.com/blog/clickfix-fake-captcha-attacks/
- https://thehackernews.com/2026/08/doublecup-uses-clickfix-and-cached-pngs.html
- https://thehackernews.com/2026/08/over-250-clickfix-domains-use-browser.html
- https://www.hexnode.com/blogs/doublecup-clickfix-browser-cache-malware-enterprise-defense/

**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

### CISA INCORPORA TRES VULNERABILIDADES AL CATÁLOGO KEV POR EXPLOTACIÓN ACTIVA (LANGFLOW, APACHE TOMCAT Y N-ABLE N-CENTRAL)

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha añadido oficialmente tres vulnerabilidades críticas a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV). Los fallos afectan a la plataforma de desarrollo de IA IBM Langflow OSS, al servidor web y de aplicaciones Apache Tomcat, y a la herramienta de monitoreo remoto N-able N-central. La inclusión se fundamenta en evidencias confirmadas de explotación activa en el entorno real por parte de actores de amenaza, incluyendo campañas automatizadas mediante inteligencia artificial y grupos de ciberespionaje vinculados a China.

**Resumen técnico:**

- Identificadores principales: CVE-2026-9198 (Langflow), CVE-2026-34486 (Apache Tomcat) y CVE-2026-18556 / CVE-2026-18577 (N-able N-central).
- Productos y versiones afectadas: * IBM Langflow OSS: Versiones 1.0.0 a 1.10.0 (Corregido en v1.10.1).
- Apache Tomcat: Versiones 11.0.20, 10.1.53 y 9.0.116 (Corregido en v11.0.21, v10.1.54 y v9.0.117).
- N-able N-central: Versiones hasta 2026.1 y 2026.3.1 (Afectado por bypass de parche inicial).
- Vectores de ataque y mecanismos de falla:
- CVE-2026-9198 (CVSS 9.8): Inyección de código en Langflow. Permite a un atacante no autenticado encadenar los puntos de enlace /api/v1/auto_login (que emite tokens de superusuario a cualquier solicitante) y /api/v1/validate/code (que ejecuta código Python arbitrario vía exec()) para lograr ejecución remota de código (RCE) en despliegues predeterminados.
- CVE-2026-34486 (CVSS 7.5): Falta de cifrado de datos sensibles en Apache Tomcat. Al corregir un fallo anterior de padding oracle, la lógica del componente EncryptInterceptor cambió a "abierto ante fallas" (fail-open), permitiendo omitir el cifrado en la comunicación entre nodos del clúster y reenviar código controlado por el atacante a la capa de deserialización.
- CVE-2026-18556 / CVE-2026-18577 (CVSS 8.2 / 8.1): Omisión de autenticación en la plataforma RMM N-able N-central. Actores maliciosos explotaron el fallo inicial como día cero para obtener acceso administrativo. La mitigación inicial fue eludida mediante la nueva falla CVE-2026-18577.

- Contexto de amenazas y actores: La explotación es activa a nivel global. La vulnerabilidad de Tomcat (CVE-2026-34486) está siendo utilizada en campañas masivas atribuidas a actores vinculados a China, que emplean agentes de IA autónomos **(**DeepSeek/Hermes Agent**)** para automatizar escaneos y ataques, además de desplegar el cargador SNOWLIGHT para Linux y herramientas como GoCobaltStrike en infraestructuras gubernamentales y empresariales.
- Plazo de cumplimiento gubernamental: Bajo la directiva BOD 26-04, CISA fijó el 07 de agosto de 2026 como fecha límite obligatoria para que las agencias federales de EE. UU. apliquen los parches correspondientes.

**Impacto potencial:**

- Toma de control total de infraestructura y servidores de aplicaciones: La ejecución remota de código en Langflow y Apache Tomcat otorga acceso sin restricciones a los sistemas subyacentes, permitiendo el robo de datos, el despliegue de malware y el control del servidor.
- Compromiso en cadena de clientes mediante plataformas RMM: Al vulnerarse N-able N-central, los atacantes obtienen acceso administrativo centralizado a la herramienta utilizada por proveedores de servicios administrados (MSPs), permitiendo la propagación lateral directa hacia las redes de múltiples empresas e industrias clientes.
- Ataques automatizados a escala masiva mediante IA: La integración de modelos de lenguaje e inteligencia artificial por parte de los atacantes acelera el reconocimiento y la ejecución de exploits, ejecutando en minutos tareas de análisis de objetivos que anteriormente tomaban días.
- Despliegue de malware avanzado y persistencia en red: Explotación observada para la instalación del loader SNOWLIGHT, herramientas de tunelizacion, implantes de Cobalt Strike y compromiso de cuentas cPanel/WHM y dominios Active Directory.

**Recomendaciones para mitigar el riesgo:**

1. Actualización prioritaria de instancias Apache Tomcat: Migrar inmediatamente las instalaciones de Apache Tomcat a las versiones parcheadas 11.0.21, 10.1.54 o 9.0.117, asegurando que los clústeres no operen bajo la configuración vulnerable de EncryptInterceptor.
2. Actualización de IBM Langflow OSS: Actualizar todos los despliegues de la herramienta de IA a la versión 1.10.1 o superior y verificar que los puntos de enlace de la API no estén expuestos directamente a redes no confiables.
3. Remediación integral en N-able N-central: Instalar los parches de emergencia más recientes emitidos por N-able para corregir tanto CVE-2026-18556 como la evasión del parche CVE-2026-18577, auditando los accesos administrativos recientes.
4. Cacería de amenazas e inspección de indicadores (IoCs): Monitorear los entornos en busca de artefactos asociados al malware SNOWLIGHT, tráfico inusual hacia marcos C2 de GoCobaltStrike, ejecuciones sospechosas de Python en entornos de IA o comportamientos anómalos en consolas RMM.

**Prioridad: Urgente.**

**Ampliar Información:**

- https://www.cisa.gov/news-events/alerts/2026/08/04/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://cyberworldops.eu/es/cisa-anade-tres-fallos-al-catalogo-kev-langflow-tomcat-y-n-central
- https://thehackernews.com/2026/08/cisa-flags-langflow-rce-tomcat-and-n.html
- https://www.securityweek.com/cisa-warns-of-exploited-langflow-n-central-and-tomcat-vulnerabilities/amp/
- https://www.diariobitcoin.com/noticias/cisa-alerta-por-tres-vulnerabilidades-explotadas-en-langflow-n-central-y-tomcat/