GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición °0126

## 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** | 1 | 0 | 0 |
| **NOTICIAS DE CIBERSEGURIDAD** | 0 | 0 | 1 |

## VULNERABILIDADES

### PLATAFORMA N8N — VULNERABILIDAD CRÍTICA "NI8MARE" DE RCE SIN AUTENTICACIÓN (CVE-2026-21858)

Investigadores de Cyera Research Labs han revelado detalles de una falla de seguridad de máxima gravedad en n8n, la plataforma de automatización de flujos de trabajo. El fallo, identificado como Ni8mare, permite a un atacante remoto no autenticado obtener control total sobre las instancias afectadas, comprometiendo la centralización de credenciales y procesos de negocio.

**Resumen técnico:**

- Identificador principal: CVE-2026-21858 (Ni8mare).
- Severidad: 10.0 (Crítica).
- Causa raíz: Defecto de "confusión de tipo de contenido" en la función parseRequestBody(), que procesa solicitudes basándose erróneamente en el encabezado Content-Type.
- Falla de lógica: El nodo formWebhook() invoca la función copyBinaryFile() para manejar archivos sin validar que el contenido sea realmente multipart/form-data.
- Mecanismo de explotación: Un atacante puede manipular el objeto req.body.files para forzar al sistema a copiar cualquier archivo local en lugar de uno cargado por el usuario.
- Vector de ataque: Ejecución remota desde la red; no requiere credenciales previas ni interacción del usuario.
- Versiones afectadas: Todas las versiones de n8n anteriores a la 1.65.0.

**Impacto potencial:**

- Lectura arbitraria de archivos: Acceso no autorizado a archivos sensibles del sistema operativo y de la aplicación.
- Exfiltración de base de datos: Robo del archivo database.sqlite, el cual contiene hashes de contraseñas, correos de administradores e IDs de usuario.
- Robo de material criptográfico: Extracción de la clave secreta de cifrado de la instancia desde los archivos de configuración.
- Bypass de autenticación: Capacidad de forjar cookies de sesión de administrador utilizando la clave de cifrado y el ID de usuario exfiltrados.
- Ejecución Remota de Código (RCE): Creación de nuevos flujos de trabajo con nodos "Execute Command" para ejecutar instrucciones a nivel de sistema operativo.
- Compromiso de ecosistemas: Acceso a servicios externos integrados (AWS, Salesforce, Google Cloud) mediante el uso de los tokens OAuth y credenciales API almacenados.

**Recomendaciones de mitigación:**

1. Actualización inmediata: Migrar de forma obligatoria a la versión 1.121.0 o versiones superiores (como la 2.3.0) para corregir el fallo de lógica.
2. Restricción de acceso: Evitar la exposición directa de la interfaz de n8n a Internet, utilizando VPNs o túneles seguros para el acceso administrativo.
3. Autenticación de formularios: Aplicar autenticación obligatoria y estricta en todos los flujos de trabajo que utilicen nodos de tipo "Form Webhook".
4. Deshabilitación de endpoints: Como medida temporal, restringir o desactivar los endpoints de webhooks y formularios que tengan acceso público.
5. Monitoreo de integridad: Supervisar ráfagas de tráfico inusuales hacia el parser de formularios y auditar accesos sospechosos al archivo de base de datos local.
6. Seguridad perimetral: Implementar reglas en el WAF para bloquear solicitudes que intenten manipular parámetros de archivos locales en peticiones de tipo formulario.

**Prioridad: Crítica.**

**Ampliar información:**

- https://thehackernews.com/2026/01/critical-n8n-vulnerability-cvss-100.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-rce-sin-autenticacion-en-plataforma-de-automatizacion-n8n/
- https://www.redeszone.net/noticias/seguridad/fallo-critico-n8n-solucion/
- https://blog.segu-info.com.ar/2026/01/otra-vulnerabilidad-critica-en-n8n.html

## ROUTERS D-LINK DSL — EXPLOTACIÓN ACTIVA DE VULNERABILIDAD ZERO-DAY (CVE-2026-0625)

Se ha reportado una campaña de explotación masiva dirigida a múltiples modelos de routers gateway D-Link que han sido catalogados como legados o "End of Life" (EoL). Al

tratarse de dispositivos antiguos que ya no reciben parches, el riesgo es permanente para las redes que aún mantienen estos equipos operativos.

**Resumen técnico:**

- Identificador principal: CVE-2026-0625.
- Severidad: 9.3 (Crítica).
- Causa raíz: Falta de sanitización de los parámetros de configuración DNS en la biblioteca CGI heredada dnscfg.cgi.
- Tipo de fallo: Inyección de comandos del sistema operativo que permite ejecutar instrucciones de shell arbitrarias.
- Estado de explotación: Confirmada la explotación activa en el mundo real observada por honeypots desde noviembre de 2025.
- Modelos confirmados: DSL-2640B (firmware ≤ 1.07), DSL-2740R (firmware < 1.17), DSL-2780B (≤ 1.01.14) y DSL-526B (≤ 2.01).

**Impacto potencial:**

- Secuestro de tráfico (DNSChanger): Los atacantes modifican los servidores DNS para redirigir silenciosamente el tráfico de los usuarios hacia sitios fraudulentos.
- Intercepción de credenciales: Capacidad de capturar nombres de usuario y contraseñas de servicios bancarios o correos electrónicos mediante sitios de phishing indetectables.
- Control Total del Host (RCE): Ejecución remota de código que permite a un atacante tomar el control administrativo del router.
- Persistencia maliciosa: Posibilidad de instalar malware que resista reinicios y permita el espionaje continuo de las comunicaciones de la red local.

- Integración en Botnets: Los dispositivos comprometidos pueden ser utilizados como nodos proxy o para lanzar ataques distribuidos de denegación de servicio (DDoS).
- Movimiento Lateral: El router puede servir como punto de entrada para escanear y atacar otros dispositivos críticos dentro de la red LAN.

**Recomendaciones de mitigación:**

1. Reemplazo de hardware: Esta es la única solución definitiva; los productos EoL no recibirán parches de seguridad por parte del fabricante.
2. Deshabilitación de gestión remota: Desactivar inmediatamente cualquier interfaz de administración expuesta hacia la WAN (Internet).
3. Restricción administrativa: Limitar el acceso a la configuración del router únicamente a través de conexiones físicas por cable (LAN).
4. Segmentación de red: Aislar el dispositivo en una VLAN separada si su retiro inmediato no es posible, para evitar el compromiso de otros equipos.
5. Rotación de credenciales: Cambiar todas las contraseñas de los servicios críticos accedidos a través de la red una vez que el equipo afectado haya sido reemplazado.
6. Auditoría de DNS: Verificar manualmente que las direcciones IP de los servidores DNS configuradas en el router coincidan con las de su proveedor de servicios legítimo.

**Prioridad: Crítica.**

**Ampliar información:**

- https://www.techradar.com/pro/security/this-critical-severity-flaw-in-d-link-dsl-gateway-devices-could-allow-for-remote-code-execution
- https://underc0de.org/foro/noticias-informaticas-120/explotan-vulnerabilidad-critica-en-routers-d-link-dsl-sin-soporte/
- https://securityaffairs.com/186616/hacking/hackers-actively-exploit-critical-rce-flaw-in-legacy-d-link-dsl-routers.html
- https://thehackernews.com/2026/01/active-exploitation-hits-legacy-d-link.html
- https://www.securityweek.com/hackers-exploit-zero-day-in-discontinued-d-link-devices/

## ADONISJS BODYPARSER — VULNERABILIDAD CRÍTICA DE ESCRITURA DE ARCHIVOS (CVE-2026-21440)

Se ha identificado una vulnerabilidad de severidad crítica en el paquete @adonisjs/bodyparser, componente central del framework AdonisJS. El fallo permite a un atacante remoto no autenticado escribir archivos arbitrarios en ubicaciones sensibles del servidor, lo que puede derivar en un compromiso total del sistema si se logran sobrescribir archivos de configuración o de ejecución.

**Resumen técnico:**

- Identificador principal: CVE-2026-21440.
- Severidad: 9.2 (Crítica).
- Componente afectado: Lógica de manejo de archivos multipart en el middleware del body parser.
- Causa raíz: Fallo de "Path Traversal" en la función MultipartFile.move(location, options).

- Mecanismo de falla: El sistema utiliza por defecto el nombre de archivo proporcionado por el cliente sin validación cuando el desarrollador omite el argumento de opciones o el saneamiento explícito.
- Vector de ataque: Envío de nombres de archivos manipulados con secuencias de salto de directorio (ej. ../../etc/passwd) a través de un endpoint de carga alcanzable.
- Versiones afectadas: Versiones ≤ 10.1.1 y ≤ 11.0.0-next.5.

**Impacto potencial:**

- Escritura arbitraria de archivos: Capacidad de guardar archivos fuera del directorio de carga designado.
- Ejecución Remota de Código (RCE): Posibilidad de sobrescribir scripts de inicio, código fuente o binarios que el sistema ejecute posteriormente.
- Compromiso de integridad: Alteración de archivos de configuración que definen el comportamiento de seguridad de la aplicación.
- Acceso administrativo persistente: Modificación de archivos de autenticación para ganar control total sobre el servidor.
- Pérdida de datos: Riesgo de sobrescribir bases de datos locales o archivos críticos del sistema operativo.
- Denegación de servicio: Inestabilidad del sistema provocada por la corrupción de archivos esenciales para el tiempo de ejecución.

**Recomendaciones de mitigación:**

1. Actualización inmediata: Migrar a las versiones parcheadas 10.1.2 o 11.0.0-next.6 de forma prioritaria.
2. Saneamiento de nombres: No confiar nunca en el nombre de archivo suministrado por el cliente; implementar rutinas de validación estrictas.
3. Generación de nombres únicos: Utilizar nombres de archivos aleatorios y únicos generados en el lado del servidor al llamar a .move().
4. Privilegios mínimos: Ejecutar los procesos de Node.js con los permisos de sistema de archivos mínimos estrictamente necesarios.
5. Filtros de aplicación: Implementar verificaciones a nivel de código para rechazar cualquier entrada que contenga secuencias como ../.
6. Defensa perimetral: Desplegar un WAF con reglas específicas para detectar patrones de "path traversal" en peticiones de datos multipart.
7. Arquitectura de contenedores: Utilizar sistemas de archivos de solo lectura para el código de la aplicación y aislar los directorios de carga.

**Prioridad: Crítica.**

**Ampliar información:**

- https://radar.offseq.com/threat/critical-adonisjs-bodyparser-flaw-cvss-92-enables--8bc97d84
- https://asec.ahnlab.com/en/91894/
- https://www.qsolit.com/cybersecurity-threat-advisory-adonisjs-bodyparser-vulnerability/
- https://smartermsp.com/cybersecurity-threat-advisory-adonisjs-bodyparser-vulnerability/
- https://thehackernews.com/2026/01/critical-adonisjs-bodyparser-flaw-cvss.html

## MALWARE

### MALWARE / CAMPAÑA PHALT#BLYX — PHISHING DIRIGIDO AL SECTOR HOTELERO (DCRAT)

Investigadores de Securonix han alertado sobre una sofisticada campaña de ingeniería social denominada PHALT#BLYX, que impacta directamente a organizaciones del sector hospitalidad en Europa. La operación utiliza técnicas de "ClickFix" para inducir a los empleados a ejecutar comandos maliciosos que despliegan el troyano de acceso remoto DCRat (DarkCrystal RAT), permitiendo a actores de amenaza, presuntamente de origen ruso, tomar control total de los sistemas de reserva y gestión.

**Resumen técnico:**

- Identificador de campaña: PHALT#BLYX.
- Malware entregado: DCRat (DarkCrystal RAT), un troyano basado en .NET con arquitectura modular.
- Vector de entrada: Correos de phishing que suplantan a Booking.com alertando sobre cancelaciones de reservas urgentes.
- Técnica de ingeniería social: Uso de señuelos "ClickFix" que simulan una Pantalla Azul de la Muerte (BSoD) de Windows para confundir al usuario.
- Mecanismo de ejecución: Engaña a la víctima para que pegue un script de PowerShell directamente en el cuadro de diálogo "Ejecutar" (Win + R).
- Técnica Living-off-the-Land (LotL): Abuso de la herramienta legítima MSBuild.exe para compilar y ejecutar código malicioso (v.proj) localmente.
- Evasión de defensas: Uso de process hollowing para inyectar el malware en el proceso legítimo aspnet_compiler.exe y operar solo en memoria.

**Impacto potencial:**

- Control Remoto Administrativo: Acceso total al host comprometido para ejecutar comandos, manipular archivos y observar el escritorio en tiempo real.
- Exfiltración de Datos Críticos: Robo de credenciales de acceso, información financiera de huéspedes y datos de tarjetas de crédito almacenados.
- Monitoreo de Actividad: Registro de pulsaciones de teclas (keylogging) y captura de pantallas de manera persistente y encubierta.
- Movimiento Lateral en la Red: Uso del equipo infectado como punto de entrada para atacar sistemas de gestión de propiedad (PMS) o bases de datos internas.
- Manipulación de Seguridad: Capacidad del malware para configurar exclusiones en Windows Defender o desactivar programas de protección si detecta privilegios de administrador.
- Infección Secundaria: Despliegue de cargas útiles adicionales, como mineros de criptomonedas o ransomware, según las órdenes del servidor C2.

**Recomendaciones de mitigación:**

1. Concientización del Personal: Educar a los empleados sobre el hecho de que Windows nunca solicita ejecutar comandos manuales de texto para reparar errores de sistema o BSoD.
2. Restricción de Binarios: Bloquear o monitorear estrictamente el uso de herramientas de desarrollo como MSBuild.exe en estaciones de trabajo de uso administrativo o recepción.
3. Hardening de PowerShell: Implementar políticas de ejecución restringidas y monitorear el uso de comandos sospechosos (ej. descargas externas seguidas de ejecución inmediata).
4. Control de Privilegios: Aplicar el principio de menor privilegio para asegurar que el personal no opere con cuentas administrativas de forma predeterminada.

5. Monitoreo de Defender: Configurar alertas automáticas en el EDR ante cualquier intento de modificación de exclusiones en Microsoft Defender vía Add-MpPreference.
6. Bloqueo de Infraestructura: Filtrar a nivel de firewall y DNS los dominios asociados a la campaña (ej. low-house[.]com, 2fa-bns[.]com, asj77[.]com).
7. Respuesta ante UAC: Instruir al personal para reportar bloqueos o ventanas emergentes de Control de Cuentas de Usuario (UAC) que aparezcan de forma repetitiva o inusual.

**Prioridad: Crítica.**

**Ampliar información:**

- https://rhisac.org/threat-intelligence/securonix-warns-of-phaltblyx-malware-campaign-targeting-hospitality-sector-via-fake-bookings/
- https://thehackernews.com/2026/01/fake-booking-emails-redirect-hotel.html
- https://underc0de.org/foro/noticias-informaticas-120/clickfix-ataca-hoteles-en-europa-con-falsas-pantallas-azules-de-windows/
- https://www.forgenex.com/public/en/blog/phalt-blyx-campa-a-de-phishing-con-falsas-reservas-hoteleras-distribuye-dcrat-mediante-p-ginas-de-bsod-falsas
- https://blog.segu-info.com.ar/2026/01/campana-de-phishing-simula-un-bsod-y.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

### GRUPO BLACK CAT — CAMPAÑA MASIVA DE MALWARE MEDIANTE SEO POISONING

El centro de respuesta a emergencias cibernéticas de China (CNCERT/CC) ha identificado una campaña de gran escala orquestada por el grupo criminal Black Cat. Esta operación utiliza técnicas avanzadas de envenenamiento de motores de búsqueda (SEO Poisoning) para posicionar sitios fraudulentos en los primeros resultados, engañando a los usuarios para que descarguen instaladores legítimos en apariencia, pero que contienen un backdoor diseñado para la vigilancia y el robo de activos financieros.

**Resumen técnico:**

- Actor de amenaza: Black Cat (activo desde 2022), especializado en campañas de robo de datos y control remoto persistente.
- Técnica de distribución: SEO Poisoning, manipulando los resultados de búsqueda (especialmente en Microsoft Bing) para colocar URLs maliciosas por encima de los sitios oficiales.
- Software suplantado: Herramientas populares como Google Chrome, Notepad++, WinSCP, QQ International, Obsidian e iTools.
- Dominios de phishing: Uso de nombres de dominio engañosos como cn-notepadplusplus[.]com, cn-winscp[.]com, cn-obsidian[.]com y dominios que imitan a GitHub como github.zh-cns[.]top.

- Cadena de infección: Descarga de un archivo ZIP -> Ejecutor de instalación -> Creación de acceso directo malicioso en el escritorio -> Ejecución de un backdoor mediante DLL Side-loading.
- Infraestructura C2: El malware establece comunicación con el servidor remoto sbido[.]com:2869 para recibir comandos y enviar datos exfiltrados.
- Segmentación regional: Fuerte enfoque inicial en usuarios de habla china (uso de dominios ".cn"), aunque la infraestructura técnica es capaz de afectar a usuarios globales.

**Impacto potencial:**

- Control Remoto (Backdoor): Instalación de un troyano de acceso que permite a los atacantes controlar el host infectado sin el conocimiento del usuario.
- Exfiltración de Datos del Navegador: Robo de historial de navegación, cookies de sesión y contraseñas almacenadas en aplicaciones como Chrome.
- Espionaje mediante Keylogging: Registro de todas las pulsaciones de teclas para capturar credenciales de acceso a redes corporativas y servicios bancarios.
- Robo de Criptoactivos: Antecedentes documentados de robo de más de $160,000 en criptomonedas mediante la suplantación de plataformas de trading como AICoin.
- Extracción de Portapapeles: Captura de la información copiada en el clipboard, permitiendo el robo de secretos industriales, llaves privadas y tokens de seguridad.
- Compromiso Masivo de Infraestructura: Se estima que el grupo ha comprometido aproximadamente 277,800 hosts en un periodo de solo dos semanas en diciembre de 2025.

**Recomendaciones para mitigar el riesgo:**

1. Descarga desde Fuentes Verificadas: Instruir estrictamente al personal para utilizar únicamente los dominios oficiales de los fabricantes de software.
2. Auditoría de Instalaciones: Supervisar la aparición inusual de archivos DLL desconocidos o accesos directos sospechosos creados tras instalar herramientas de terceros.
3. Seguridad DNS: Implementar soluciones de filtrado DNS que bloqueen el acceso a dominios fraudulentos y conocidos por distribuir malware.
4. Uso de EDR/AV: Desplegar soluciones de seguridad en endpoints capaces de detectar comportamientos de inyección de código y DLL Side-loading.
5. Educación sobre Buscadores: Advertir a los usuarios que los primeros resultados de búsqueda etiquetados como "Anuncios" o resultados patrocinados pueden ser maliciosos.
6. Validación de Firmas Digitales: Verificar siempre que los instaladores descargados posean una firma digital válida y reconocida del desarrollador original.
7. Bloqueo de IoCs: Integrar en los sistemas de protección perimetral los dominios y la IP del servidor C2 asociados a la infraestructura de Black Cat.

**Prioridad: Importante.**

**Ampliar Información:**

- https://thehackernews.com/2026/01/black-cat-behind-seo-poisoning-malware.html
- https://darknetsearch.com/knowledge/news/en/seo-poisoning-malware-revealed-7-key-facts-about-black-cat-operations/
- https://the420.in/black-cat-seo-poisoning-malware-fake-software-downloads-china/