GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º0526

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

SOLARWINDS WEB HELP DESK — MÚLTIPLES VULNERABILIDADES CRÍTICAS Y RCE (CVE-2025-40551)

SolarWinds ha lanzado una actualización de seguridad urgente tras la divulgación de seis vulnerabilidades en su plataforma Web Help Desk (WHD). La más crítica permite a atacantes remotos no autenticados ejecutar código arbitrario (RCE) mediante la deserialización de datos no confiables. Este fallo es especialmente peligroso debido a su alta confiabilidad para los atacantes y la ausencia de barreras de autenticación.

Resumen técnico:

- Identificador principal: CVE-2025-40551 (vinculado a CVE-2025-40536, CVE-2025-40552, CVE-2025-40553).
- Severidad: 9.8 (Crítica).
- Causa raíz: Deserialización de datos no confiables en la funcionalidad AjaxProxy y omisión de controles de seguridad (Security Protection Bypass).
- Mecanismo de falla: El atacante puede encadenar un bypass de CSRF (añadiendo parámetros falsos como /ajax/ en la URL) para acceder a componentes restringidos y luego inyectar objetos Java maliciosos a través del puente JSONRPC.
- Estado de explotación: Confirmada en el mundo real; incluida en el catálogo KEV de CISA el 3 de febrero de 2026, con fecha límite de remediación al 6 de febrero de 2026.
- Versiones afectadas: SolarWinds Web Help Desk 12.8.8 HF1 y todas las versiones anteriores.

Impacto potencial

- Ejecución Remota de Código (RCE): Capacidad para ejecutar comandos a nivel de sistema operativo en el host con privilegios totales.
- Invocación de acciones restringidas: Los fallos de bypass de autenticación (CVE-2025-40552/4) permiten ejecutar métodos protegidos y funciones administrativas sin credenciales.
- Acceso a datos sensibles: Compromiso de tickets de soporte, inventarios de hardware/software y posibles credenciales almacenadas en la plataforma de gestión.

Recomendaciones de mitigación:

1. Actualización obligatoria: Migrar de forma inmediata a la versión SolarWinds WHD 2026.1.
2. Restricción perimetral: Bloquear el acceso externo a la ruta URI /helpdesk/WebObjects/ y limitar el uso de la herramienta a redes internas o VPN.
3. Implementación de firmas IPS: Aplicar firmas específicas (ej. SonicWall IPS 21895/21896) para detectar intentos de explotación de deserialización y bypas

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/01/solarwinds-fixes-four-critical-web-help.html
- https://thehackernews.com/2026/02/cisa-adds-actively-exploited-solarwinds.html
- https://socradar.io/blog/solarwinds-web-help-desk-rce-auth-bypass-bugs/
- https://www.sonicwall.com/blog/multiple-vulnerabilities-in-solarwinds-web-help-desk-leading-to-rce-cve-2025-40551
- https://techconsulting.es/vulnerabilidades-y-avisos-de-seguridad-multiples-vulnerabilidades-en-web-help-desk-de-solarwinds/

METRO4SHELL — EJECUCIÓN REMOTA DE CÓDIGO (RCE) EN SERVIDOR METRO (CVE-2025-11953)

Se ha detectado la explotación activa de una vulnerabilidad crítica en el servidor de desarrollo Metro, incluido en el paquete npm @react-native-community/cli. El fallo permite a atacantes remotos no autenticados ejecutar comandos arbitrarios en el sistema operativo del host (estaciones de trabajo de desarrolladores o agentes de CI/CD) mediante solicitudes POST manipuladas al endpoint /open-url.

Resumen técnico:

- Identificador principal: CVE-2025-11953 (Metro4Shell).
- Severidad: 9.8 (Crítica).
- Causa raíz: Inyección de comandos del sistema operativo (CWE-78) debido a una sanitización insuficiente de la entrada del usuario en el componente cli-server-api.
- Mecanismo de falla: El servidor Metro, al no estar restringido por defecto a localhost, procesa comandos enviados en el cuerpo de una petición JSON, permitiendo el despliegue de scripts maliciosos.
- Estado de explotación: Confirmada y persistente en el mundo real. Se han observado ataques desde diciembre de 2025 que utilizan scripts de PowerShell base64 para evadir defensas.
- Versiones afectadas: Versiones de @react-native-community/cli-server-api desde la 4.8.0 hasta versiones anteriores a la 18.0.1, 19.1.2 y 20.0.0.

Impacto potencial

- Compromiso del entorno de desarrollo: Ejecución de binarios basados en Rust con capacidades de persistencia y técnicas de anti-análisis en el equipo del desarrollador.
- Evasión de Antivirus: Los exploits observados utilizan comandos de PowerShell para añadir exclusiones en Microsoft Defender sobre directorios críticos (AppData\Local\Temp), facilitando la infección.
- Robo de Propiedad Intelectual: Acceso no autorizado al código fuente, variables de entorno, llaves de API y secretos de producción almacenados en el entorno de compilación.
- Ataques a la Cadena de Suministro: Posibilidad de inyectar código malicioso en las aplicaciones móviles durante el proceso de empaquetado (bundling) antes de ser publicadas.

Recomendaciones de mitigación:

1. Actualización Urgente: Actualizar @react-native-community/cli-server-api a las versiones corregidas (18.0.1, 19.1.2 o 20.0.0). Verificar versiones globales y locales con npm list.
2. Configuración de Binding: Forzar al servidor Metro a vincularse únicamente a la interfaz local utilizando el parámetro --host 127.0.0.1 en los scripts de inicio.
3. Segmentación de Red: Implementar reglas de firewall de host para bloquear el tráfico entrante al puerto 8081 desde cualquier red externa o segmentos de red no confiables.
4. Detección de Amenazas: Configurar reglas en EDR/XDR para alertar sobre solicitudes POST inusuales hacia /open-url y la ejecución de procesos hijos sospechosos desde node.exe.

Prioridad: Crítica.

Ampliar información:

- https://www.vulncheck.com/blog/metro4shell_eitw
- https://socradar.io/blog/cve-2025-11953-metro4shell-react-native-metro-rce/
- https://unaaldia.hispasec.com/2026/02/exploit-activo-de-metro4shell-servidores-de-desarrollo-comprometidos-via-rce-en-react-native.html
- https://thehackernews.com/2026/02/hackers-exploit-metro4shell-rce-flaw-in.html

IVANTI EPMM — EJECUCIÓN REMOTA DE CÓDIGO (RCE) EXPLOTADA COMO ZERO-DAY (CVE-2026-1281 & CVE-2026-1340)

Ivanti ha divulgado dos vulnerabilidades críticas de inyección de código en su solución de gestión de dispositivos móviles Endpoint Manager Mobile (EPMM). Estos fallos permiten a un atacante remoto no autenticado ejecutar comandos arbitrarios en el servidor afectado mediante solicitudes HTTP GET especialmente diseñadas. CISA ha incluido estos fallos en su catálogo KEV, confirmando su explotación activa en ataques dirigidos.

Resumen técnico:

- Identificadores principales: CVE-2026-1281 y CVE-2026-1340.
- Severidad: 9.8 (Crítica).
- Causa raíz: Control inadecuado de la generación de código (CWE-94) en los scripts de Bash encargados de procesar la distribución de aplicaciones internas y configuraciones de transferencia de archivos.
- Mecanismo de falla: El atacante puede inyectar comandos de Bash a través de parámetros en las URLs de los endpoints /mifs/c/appstore/fob/ y /mifs/c/aftstore/fob/. El servidor ejecuta estos comandos con privilegios de sistema.
- Estado de explotación: Confirmada como Zero-Day. Explotada activamente antes de su divulgación oficial. CISA estableció una fecha límite de remediación de solo 3 días (1 de febrero de 2026) para agencias gubernamentales.
- Versiones afectadas: Versiones 12.7.0.0, 12.6.1.0, 12.5.1.0 y todas las versiones anteriores de las ramas 12.x.

Impacto potencial:

- Acceso a Datos Sensibles (PII): El compromiso del servidor EPMM otorga acceso a nombres, correos electrónicos, números de teléfono y coordenadas GPS de todos los dispositivos móviles gestionados.
- Persistencia mediante Web Shells: Los atacantes han sido observados desplegando shells reversos y web shells para mantener el acceso persistente incluso después de reinicios del sistema.
- Movimiento Lateral: Dada la ubicación privilegiada de EPMM en la red, un atacante puede utilizar el servidor comprometido como puente para saltar hacia la infraestructura interna de la organización.
- Compromiso Total del Dispositivo: Ejecución de código arbitrario con privilegios de root, permitiendo la modificación de políticas de seguridad y la interceptación de comunicaciones de los dispositivos enrolados.

Recomendaciones de mitigación:

1. Actualización de Emergencia: Aplicar inmediatamente el parche RPM correspondiente (12.x.0.x o 12.x.1.x) según la versión instalada. Nota: El parche debe reaplicarse si se realiza un upgrade de versión posterior.
2. Búsqueda de Compromiso (Threat Hunting): Revisar los logs de acceso de Apache (/var/log/httpd/https-access_log) utilizando la expresión regular: ^(?!127\.0\.0\.1:\d+ .*$).*?\/mifs\/c\/(aft|app)store\/fob\/.*?404.
3. Auditoría de Cuentas y Políticas: Verificar la creación de nuevos administradores locales, cambios en configuraciones de SSO/LDAP y aplicaciones "push" recientemente añadidas que no hayan sido autorizadas.
4. Restauración en Caso de Infección: Si se detectan indicadores de compromiso (IoCs), se recomienda reconstruir el servidor EPMM desde una copia de seguridad limpia o una instalación nueva antes de migrar los datos.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/01/two-ivanti-epmm-zero-day-rce-flaws.html
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US
- https://cibersafety.com/vulnerabilidades-criticas-cve-ivanti-epmm/
- https://www.rapid7.com/blog/post/etr-critical-ivanti-endpoint-manager-mobile-epmm-zero-day-exploited-in-the-wild-eitw-cve-2026-1281-1340/

MALWARE

DEAD#VAX — DESPLIEGUE DE ASYNCRAT MEDIANTE ABUSO DE IPFS Y VHD

Se ha identificado una sofisticada campaña de malware denominada DEAD#VAX, la cual utiliza técnicas avanzadas de evasión para desplegar el troyano de acceso remoto AsyncRAT. La campaña destaca por el uso de archivos de imagen de disco virtual (VHD) alojados en la red descentralizada IPFS y una cadena de ejecución que ocurre enteramente en memoria, evitando dejar rastros en el disco físico del sistema comprometido.

Resumen técnico:

- Tipo de amenaza: Troyano de Acceso Remoto (RAT) / Malware Fileless.
- Vector de ataque: Phishing dirigido con archivos VHD disfrazados de facturas o documentos PDF legítimos.
- Mecanismo de infección: El ataque utiliza una cadena de múltiples etapas: un archivo de script de Windows (WSF) inicia un script de procesamiento por lotes (batch) altamente ofuscado, que a su vez carga un inyector de procesos basado en PowerShell.
- Técnica de evasión: Uso de VHD para eludir la marca de la web (MotW) y escaneos de correo tradicionales. El payload final se inyecta como shellcode x64 directamente en procesos firmados por Microsoft (como OneDrive.exe o RuntimeBroker.exe).
- Infraestructura: Aloja sus artefactos iniciales en el sistema de archivos interplanetario (IPFS), lo que dificulta el derribo (takedown) de los servidores de descarga.

Impacto potencial:

- Control Total del Endpoint: AsyncRAT permite la vigilancia a largo plazo, incluyendo la captura de pantalla, activación de cámara web y registro de pulsaciones de teclas (keylogging).
- Exfiltración de Datos: Capacidad para navegar por el sistema de archivos, robar credenciales del portapapeles y extraer documentos sensibles de la organización.
- Dificultad Forense: Al ejecutarse exclusivamente en memoria y utilizar scripts que se autodestruyen o se ofuscan en tiempo de ejecución, la reconstrucción del incidente tras un reinicio es extremadamente compleja.
- Persistencia Sigilosa: Implementa tareas programadas y lanzadores basados en scripts que rotan automáticamente, evitando los indicadores comunes de persistencia en el registro de Windows.

Recomendaciones de mitigación:

1. Bloqueo de Extensiones: Restringir el montaje de archivos .vhd y .vhdx en estaciones de trabajo de usuarios finales a menos que sea estrictamente necesario para su labor.
2. Filtrado de Correo: Configurar las pasarelas de seguridad (Secure Email Gateways) para inspeccionar y bloquear correos electrónicos que contengan enlaces a dominios de gateways de IPFS (ej. ipfs.io, pinata.cloud).
3. Monitoreo de Procesos: Implementar reglas de EDR para detectar la inyección de código en procesos legítimos de Windows y el uso inusual de scripts (WSF, PowerShell) con altos niveles de ofuscación o entropía.
4. Hardening de PowerShell: Habilitar el registro de bloques de scripts (Script Block Logging) y el modo de lenguaje restringido (Constrained Language Mode) para limitar la capacidad de ejecución de cargadores maliciosos.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/02/deadvax-malware-campaign-deploys.html
- https://siliconangle.com/2026/02/04/securonix-warns-deadvax-malware-campaign-abusing-windows-fileless-execution/
- https://www.socdefenders.ai/item/086ba026-ddb0-409c-af7c-38112149a249

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

MICROSOFT DESARROLLA ESCÁNER PARA DETECTAR "SLEEPER AGENTS" EN MODELOS DE LENGUAJE (LLM)

Microsoft ha anunciado la creación de un nuevo escáner ligero diseñado para identificar puertas traseras ("backdoors") en modelos de IA de pesos abiertos (open-weight). Esta herramienta busca combatir el "envenenamiento de modelos", un ataque donde se entrena a la IA para actuar de forma maliciosa solo ante disparadores específicos, permaneciendo inactiva y pareciendo inofensiva en situaciones normales.

Resumen técnico:

- Tipo de tecnología: Escáner de seguridad para Modelos de Lenguaje Extensos (LLM).
- Capacidad de detección: Identifica "sleeper agents" basándose en tres señales observables: patrones de atención "double triangle", fuga de datos por memorización y activación por disparadores difusos.
- Mecanismo de falla: El envenenamiento ocurre en los pesos del modelo durante el entrenamiento, creando una instrucción condicional oculta que no requiere ejecución de código malicioso tradicional.
- Alcance: Funciona en modelos de estilo GPT y no requiere conocimiento previo del disparador ni entrenamiento adicional.

Impacto potencial:

- Confianza en el suministro de IA: Permite a las empresas auditar modelos de código abierto (como los de Hugging Face) antes de integrarlos en sus operaciones.
- Prevención de fugas de datos: El escáner detecta si el modelo tiende a "regurgitar" datos sensibles usados durante su manipulación.
- Mitigación de ataques encubiertos: Identifica comportamientos que podrían estar diseñados para activarse solo en entornos de producción específicos.
- Resiliencia del ecosistema: Fomenta un estándar de seguridad auditable para modelos que tradicionalmente se consideran "cajas negras".

Recomendaciones para mitigar el riesgo:

1. Integración en SDL: Incorporar el escaneo de modelos como una fase obligatoria en el Ciclo de Vida de Desarrollo Seguro (SDL) de aplicaciones con IA.
2. Auditoría de pesos abiertos: Utilizar esta herramienta específicamente para modelos descargados cuyos pesos sean accesibles para análisis local.
3. Defensa en profundidad: No depender únicamente del escáner; complementar con red-teaming de IA y monitoreo de las salidas en tiempo real.
4. Evaluación de procedencia: Verificar siempre la integridad de la cadena de suministro de los modelos, priorizando repositorios y firmas verificadas.

Prioridad: Importante.

Ampliar Información:

- https://www.microsoft.com/en-us/security/blog/2026/02/04/detecting-backdoored-language-models-at-scale/
- https://thehackernews.com/2026/02/microsoft-develops-scanner-to-detect.html
- https://www.zdnet.com/article/ai-model-poisoned-warning-signs/
- https://www.socdefenders.ai/item/2aa70505-31e3-4eb1-baf3-a59c03b66270