GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0426

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

VULNERABILIDADES

PRODUCTOS FORTINET — BYPASS DE AUTENTICACIÓN CRÍTICO EN FORTICLOUD SSO (CVE-2026-24858)

Fortinet ha confirmado una vulnerabilidad de omisión de autenticación de severidad crítica que afecta a la funcionalidad FortiCloud SSO. El fallo permite a un atacante que posea una cuenta de FortiCloud y un dispositivo registrado acceder de forma no autorizada a otros dispositivos asociados a cuentas diferentes, siempre que el inicio de sesión vía SSO esté habilitado. La vulnerabilidad está siendo explotada activamente para crear cuentas de administrador locales y exfiltrar archivos de configuración.

Resumen técnico:

- Identificador principal: CVE-2026-24858.
- Severidad: 9.4 (Crítica).
- Causa raíz: Uso de un canal o vía alterna para la autenticación (CWE-288) en el componente de la interfaz gráfica (GUI).
- Estado de explotación: Confirmada en el mundo real; incluida en el catálogo KEV de CISA con fecha límite de remediación al 30 de enero de 2026.
- Versiones afectadas:
- FortiOS: Ramas 7.0 (hasta 7.0.18), 7.2 (hasta 7.2.12), 7.4 (hasta 7.4.10) y 7.6 (hasta 7.6.5).
- FortiManager/FortiAnalyzer: Ramas 7.0 a 7.6.
- FortiProxy: Versiones 7.0 y 7.2 (todas), 7.4 y 7.6.
- FortiWeb: Ramas 7.4, 7.6 y 8.0.

Impacto potencial:

- Compromiso total del dispositivo: El atacante puede eludir el inicio de sesión y obtener control administrativo sobre el hardware.
- Persistencia encubierta: Se ha observado la creación de cuentas locales con nombres como audit, itadmin, backup, support o secadmin para mantener el acceso tras el cierre de la brecha inicial.
- Robo de secretos: Descarga del archivo de configuración del sistema (config file), lo que expone credenciales y topologías de red.

Recomendaciones de mitigación:

1. Actualización obligatoria: Migrar de forma inmediata a las versiones corregidas (ej. FortiOS 7.4.11+, FortiAnalyzer 7.4.10+). Fortinet ya no permite conexiones SSO desde versiones vulnerables.
2. Búsqueda de IoCs: Auditar logs en busca de inicios de sesión exitosos desde las cuentas maliciosas cloud-noc@mail.io y cloud-init@mail.io.
3. Auditoría de cuentas: Verificar la existencia de usuarios administradores creados recientemente que no correspondan al equipo oficial.
4. Medida preventiva (CLI): Aunque el fabricante bloqueó el SSO de forma centralizada para versiones antiguas, se recomienda deshabilitarlo localmente: config system global -> set admin-forticloud-sso-login disable.

Prioridad: Crítica.

Ampliar información:

- https://www.fortiguard.com/psirt/FG-IR-26-060
- https://s2grupo.es/vulnerabilidades-criticas-fortinet-2026/
- https://socprime.com/es/blog/cve-2026-24858-vulnerabilidad/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-bypass-de-autenticacion-en-fortinet-forticloud-sso-cve-2026-24858/

LIBRERÍA VM2 PARA NODE.JS — FALLO CRÍTICO DE ESCAPE DE SANDBOX (CVE-2026-22709)

Se ha divulgado una vulnerabilidad crítica en vm2, una de las librerías de sandboxing más utilizadas para el entorno Node.js. El fallo permite a un atacante eludir por completo las protecciones de aislamiento y ejecutar código arbitrario directamente en el sistema operativo host. Esta vulnerabilidad es especialmente preocupante dado que el propósito principal de esta librería es, precisamente, servir como una barrera de seguridad para ejecutar código no confiable.

Resumen técnico:

- Identificador principal: CVE-2026-22709.
- Severidad: 9.8 (Crítica).
- Causa raíz: Sanitización inadecuada de los controladores de "Promises" (CWE-693).
- Mecanismo de falla: El fallo reside en que las funciones asíncronas en JavaScript devuelven objetos globalPromise (del entorno host) en lugar de localPromise (del sandbox). Debido a que los prototipos de globalPromise no están debidamente protegidos, un atacante puede interceptar el método .call() y escalar a través de la cadena de prototipos hasta obtener el constructor de Function del sistema principal.
- Vector de ataque: Acceso a través de la red; baja complejidad técnica. No requiere privilegios previos ni interacción por parte del usuario.
- Versiones afectadas: Todas las versiones iguales o anteriores a la 3.10.1.

Impacto potencial:

- Ejecución Remota de Código (RCE): El atacante puede ejecutar comandos con los mismos privilegios que la aplicación Node.js, permitiendo el control total del servidor.
- Acceso al sistema de archivos: Capacidad para leer, modificar o eliminar archivos fuera del entorno restringido del sandbox.
- Exfiltración de datos: Acceso a variables de entorno, claves de API y bases de datos a las que el proceso principal tenga acceso.

Recomendaciones de mitigación:

1. Actualización urgente: Migrar inmediatamente a la versión 3.10.3, la cual reemplaza el uso de Function.prototype.call() por Reflect.apply() para evitar interceptaciones.
2. Auditoría de dependencias: Revisar proyectos que utilicen paquetes como auth0-source-control-extension o herramientas de ejecución de scripts que dependan directamente de vm2.
3. Evaluación de alternativas: Dado el historial recurrente de fallos de escape en esta librería (más de 20 en los últimos años), se recomienda evaluar soluciones de aislamiento más robustas a nivel de proceso o contenedor, como isolated-vm o Docker.

Prioridad: Crítica.

Ampliar información:

- https://www.scworld.com/brief/critical-vm2-vulnerability-allows-sandbox-escape-and-arbitrary-code-execution
- https://www.endorlabs.com/learn/cve-2026-22709-critical-sandbox-escape-in-vm2-enables-arbitrary-code-execution
- https://thehackernews.com/2026/01/critical-vm2-nodejs-flaw-allows-sandbox.html
- https://www.csoonline.com/article/4123782/critical-bug-in-popular-vm2-node-js-sandboxing-library-puts-projects-at-risk.html

PRODUCTO GNU INETUTILS — OMISIÓN DE AUTENTICACIÓN REMOTA Y ACCESO ROOT (CVE-2026-24061)

Se ha descubierto una vulnerabilidad crítica en el demonio de Telnet de GNU InetUtils que permite a un atacante remoto eludir por completo el proceso de inicio de sesión y obtener acceso directo como superusuario (root). El fallo, que ha estado presente en el código desde 2015, está siendo explotado activamente en campañas coordinadas para desplegar malware y establecer persistencia en servidores Linux y Unix.

Resumen técnico:

- Identificador principal: CVE-2026-24061.
- Severidad: 9.8 (Crítica).
- Causa raíz: Inyección de argumentos mediante variables de entorno no sanitizadas (CWE-88).
- Mecanismo de falla: El servidor telnetd toma la variable de entorno USER enviada por el cliente y la pasa directamente al programa /usr/bin/login. Al enviar una cadena específicamente diseñada como -f root, el programa de login interpreta el parámetro -f como una instrucción para omitir la autenticación, otorgando una terminal de root de forma inmediata.
- Estado de explotación: Incluida en el catálogo KEV de CISA tras detectarse ataques desde múltiples direcciones IP maliciosas que realizan reconocimiento y despliegue de llaves SSH.
- Versiones afectadas: Todas las versiones de GNU InetUtils desde la 1.9.3 hasta la 2.7 inclusive (distribuciones como Debian, Ubuntu y Kali son vulnerables si tienen este paquete instalado).

Impacto potencial:

- Acceso administrativo total: Obtención de una consola con privilegios de root sin necesidad de conocer contraseñas.
- Ejecución de código arbitrario: Capacidad para ejecutar comandos del sistema, instalar herramientas de hacking o manipular servicios críticos.
- Establecimiento de persistencia: Los atacantes están utilizando este acceso para inyectar llaves SSH y garantizar el reingreso al sistema incluso si se cierra el servicio Telnet.
- Compromiso de la tríada CIA: El atacante tiene control total para leer datos sensibles (Confidencialidad), modificar registros (Integridad) o cifrar el sistema (Disponibilidad).

Recomendaciones de mitigación:

1. Actualización del paquete: Migrar de forma inmediata a GNU InetUtils 2.8 o aplicar los parches específicos de seguridad de su distribución de Linux.
2. Desactivación del servicio: Se recomienda encarecidamente deshabilitar el demonio telnetd y reemplazarlo por protocolos seguros y cifrados como SSH.
3. Restricción perimetral: Bloquear o restringir el acceso al puerto TCP/23 mediante firewalls, permitiendo únicamente conexiones desde redes de gestión confiables o vía VPN.
4. Auditoría de logs y sistemas: Revisar los registros de autenticación en busca de accesos anómalos de root y verificar el archivo ~/.ssh/authorized_keys para detectar llaves no autorizadas.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/01/critical-gnu-inetutils-telnetd-flaw.html
- https://nsfocusglobal.com/gnu-inetutils-telnetd-remote-authentication-bypass-vulnerability-cve-2026-24061-notice/
- https://www.yorku.ca/uit/2026/01/gnu-inetutils-telnetd-authentication-bypass-cve-2026-24061/
- https://ccb.belgium.be/advisories/warning-critical-authentication-bypass-gnu-inetutils-telnetd-patch-immediately

WINRAR — EXPLOTACIÓN MASIVA DE VULNERABILIDAD DE TRAVERSAL DE RUTA (CVE-2025-8088)

Google Threat Intelligence Group ha advertido sobre la explotación activa y generalizada de una vulnerabilidad de severidad alta en WinRAR. El fallo permite a diversos actores de amenazas, tanto estatales como con fines financieros, depositar archivos maliciosos en carpetas críticas del sistema para obtener persistencia automática. A pesar de contar con un parche desde mediados de 2025, la lentitud en la actualización de este software ha permitido que grupos vinculados a Rusia y China sigan utilizándolo con éxito.

Resumen técnico:

- Identificador principal: CVE-2025-8088.
- Severidad: 8.8 (Alta).
- Causa raíz: Validación insuficiente de nombres de flujo en Alternate Data Streams (ADS) combinada con secuencias de salto de directorio (CWE-22).
- Mecanismo de falla: El atacante crea un archivo RAR que contiene un documento señuelo (ej. un PDF). Oculto en los flujos de datos alternos (ADS) del archivo, se incluye un payload (como un acceso directo .LNK) con una ruta de extracción manipulada (ej. ../../AppData/Roaming/.../Startup/). Al descomprimir el archivo, WinRAR extrae silenciosamente el componente malicioso en la carpeta de Inicio de Windows.
- Actores identificados: Grupos como APT44 (Sandworm), Turla, RomCom y diversos actores con fines financieros que distribuyen RATs como AsyncRAT y XWorm.

Impacto potencial:

- Persistencia en el arranque: Al depositar archivos en la carpeta de "Startup", el malware se ejecuta automáticamente cada vez que el usuario inicia sesión sin necesidad de interacción adicional.
- Ejecución de código arbitrario: Permite el despliegue de troyanos de acceso remoto (RAT) y scripts maliciosos que otorgan control total sobre la estación de trabajo.
- Espionaje y exfiltración: Grupos de APT han utilizado este vector para desplegar suites de malware especializadas en el robo de documentos militares y gubernamentales.
- Inyección de phishing bancario: Se han detectado campañas dirigidas a usuarios financieros donde se instalan extensiones de navegador maliciosas para interceptar credenciales bancarias.

Recomendaciones de mitigación:

1. Actualización obligatoria: Actualizar de forma inmediata todas las instalaciones de WinRAR a la versión 7.13 o superior, la cual corrige la gestión de flujos ADS.
2. Monitoreo de rutas críticas: Implementar reglas de detección para identificar la creación de archivos (.LNK, .HTA, .BAT, .CMD) en la carpeta de inicio (%AppData%\Microsoft\Windows\Start Menu\Programs\Startup) originados por procesos de descompresión.
3. Control de aplicaciones: Utilizar políticas de "AppLocker" o "Windows Defender Application Control" para impedir la ejecución de scripts o binarios no firmados desde directorios temporales o de inicio.
4. Escaneo de archivos adjuntos: Configurar las soluciones de seguridad perimetral y de correo electrónico para bloquear o inspeccionar archivos RAR que contengan múltiples flujos de datos (ADS) o rutas de archivo inusuales.

Prioridad: Urgente.

Ampliar información:

- https://socprime.com/active-threats/cve-2025-8088-critical-winrar-vulnerability/
- https://thehackernews.com/2026/01/google-warns-of-active-exploitation-of.html
- https://cloud.google.com/blog/topics/threat-intelligence/exploiting-critical-winrar-vulnerability

MALWARE

FALSA EXTENSIÓN DE IA PARA VS CODE (MOLTBOT / CLAWDBOT) — DESPLIEGUE DE MALWARE DE ACCESO REMOTO

Investigadores de seguridad han detectado una campaña de ataque a la cadena de suministro que utiliza el Marketplace oficial de Visual Studio Code para distribuir una extensión maliciosa. Los atacantes suplantaron la identidad del popular proyecto de código abierto Moltbot (anteriormente conocido como Clawdbot), ofreciendo un asistente de codificación gratuito que, en realidad, despliega herramientas de acceso remoto para tomar control de las estaciones de trabajo de los desarrolladores.

Resumen técnico:

- Nombre de la amenaza: ClawdBot Agent - AI Coding Assistant.
- Identificador de la extensión: clawdbot.clawdbot-agent.
- Mecanismo de infección: La extensión se ejecuta automáticamente cada vez que se inicia el entorno de desarrollo (IDE). Tras activarse, descarga un archivo de configuración (config.json) que instruye la ejecución de un binario malicioso denominado Code.exe.
- Carga útil (Payload): El malware instala una instancia preconfigurada de ConnectWise ScreenConnect, un software legítimo de administración remota, configurado para conectarse al servidor del atacante en meeting.bulletmailer[.]net:8041.
- Técnicas de evasión: Incluye mecanismos de redundancia mediante el uso de DLL Sideloading (utilizando una DLL escrita en Rust llamada DWrite.dll) y descarga de componentes desde servicios en la nube como Dropbox, asegurando la infección incluso si la infraestructura principal es bloqueada.

Impacto potencial:

- Acceso remoto persistente: Los atacantes obtienen control total y silencioso de la máquina afectada mediante el cliente de ScreenConnect, permitiendo el movimiento lateral en la red corporativa.
- Exfiltración de secretos y credenciales: Robo de llaves de API (OpenAI, Anthropic), tokens de acceso, secretos de entorno (.env) y bases de datos locales utilizadas en el desarrollo.
- Exposición de datos privados: Acceso a historiales de chat, configuraciones de OAuth y datos de mensajería integrados (Slack, Teams, WhatsApp) que el asistente de IA gestiona de forma legítima.
- Suplantación de identidad: Capacidad del atacante para enviar mensajes o inyectar código en nombre del desarrollador a través de las plataformas de comunicación conectadas.

Recomendaciones de mitigación:

1. Desinstalación inmediata: Eliminar la extensión clawdbot.clawdbot-agent y realizar un escaneo completo de procesos en busca de instancias no autorizadas de ScreenConnect.
2. Bloqueo de red: Restringir el tráfico saliente hacia los dominios identificados: clawdbot.getintwopc[.]site, meeting.bulletmailer[.]net y darkgptprivate[.]com.
3. Revocación de secretos: Invalidar y rotar todas las llaves de API y credenciales que estuvieran configuradas en el entorno de VS Code o en las variables de entorno del sistema comprometido.
4. Políticas de Marketplace: Implementar listas blancas (allow-lists) en la organización para restringir la instalación de extensiones de VS Code únicamente a editores verificados y software aprobado.
5. Auditoría de "Skills": Si se utiliza la versión legítima de Moltbot, revisar exhaustivamente las integraciones y evitar la instalación de extensiones de terceros desde repositorios no oficiales como MoltHub.

Prioridad: Urgente.

Ampliar información:

- https://www.ctrlaltnod.com/news/fake-ai-extension-infiltrates-vs-code-with-remote-access-malware/#google_vignette
- https://arstechnica.com/ai/2026/01/viral-ai-assistant-moltbot-rapidly-gains-popularity-but-poses-security-risks/
- https://thehackernews.com/2026/01/fake-moltbot-ai-coding-assistant-on-vs.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

ATAQUE DE GRUPO SANDWORM CONTRA LA RED ELÉCTRICA DE POLONIA — USO DE MALWARE "DYNOWIPER"

Durante la última semana de diciembre de 2025, la infraestructura energética de Polonia fue blanco de un sofisticado intento de sabotaje digital atribuido al grupo APT Sandworm (vinculado a la inteligencia militar rusa). El ataque utilizó un nuevo malware destructivo de tipo wiper, denominado DynoWiper, con el objetivo de interrumpir las comunicaciones entre las plantas de energía renovable y los operadores de distribución eléctrica nacionales. Aunque las defensas polacas lograron neutralizar la amenaza antes de que ocurriera un apagón, el incidente marca una escalada en la guerra híbrida contra miembros de la OTAN.

Resumen técnico:

- Actor de amenaza: Sandworm (también conocido como APT44, ELECTRUM o Iridium).
- Tipo de ataque: Sabotaje contra Sistemas de Control Industrial (ICS) mediante el uso de wipers personalizados.
- Malware identificado: DynoWiper (detectado como Win32/KillFiles.NMO), diseñado para borrar datos de forma permanente y dejar los servidores inutilizados.
- Contexto histórico: El ataque fue coordinado para coincidir con el décimo aniversario del apagón de Ucrania en 2015, el primer incidente histórico de interrupción eléctrica causado por malware.
- Objetivo estratégico: Atacar nodos clave de energía renovable (parques eólicos y plantas de cogeneración) para debilitar la retaguardia energética que Polonia brinda a Ucrania.

Impacto potencial:

- Terror térmico y social: Un apagón exitoso habría dejado a más de 500,000 hogares sin calefacción ni electricidad en una de las semanas más frías del año.
- Destrucción permanente de activos: A diferencia de un ataque de ransomware, el uso de un wiper busca la inutilización física y lógica de los servidores de control, obligando a una reconstrucción total del sistema.
- Inestabilidad de la red nacional: La desconexión forzada de fuentes de energía renovable puede provocar desequilibrios de carga en la red eléctrica, causando fallos en cascada en otras subestaciones.
- Debilitamiento de alianzas regionales: Al atacar la infraestructura polaca, el agresor busca degradar la capacidad de Polonia para suministrar y recibir electricidad desde Ucrania en situaciones críticas.

Recomendaciones para mitigar el riesgo:

1. Segmentación de red (Zero Trust): Aislar estrictamente las redes de TI corporativas de las redes de tecnología operativa (OT) para evitar que el malware se propague a los sistemas de control industrial.
2. Monitoreo preventivo de APTs: Implementar soluciones de detección de amenazas que busquen indicadores específicos asociados a Sandworm, especialmente aquellos que involucran manipulación de protocolos industriales.
3. Resiliencia y Recuperación (BCP/DRP): Testear y actualizar los planes de continuidad de negocio y recuperación ante desastres, priorizando la restauración desde copias de seguridad fuera de línea (offline) inmunes a wipers.
4. Auditoría de suministros renovables: Fortalecer la seguridad en las comunicaciones entre instalaciones de energía limpia de terceros y los centros de despacho nacionales, verificando la integridad de cada nodo de conexión.

Prioridad: Urgente.

Ampliar Información:

- https://www.xataka.com/energia/regreso-sandworm-grupo-elite-gru-ruso-traslada-su-guerra-red-electrica-ucrania-a-suelo-polaco/amp
- https://attack.mitre.org/groups/G0034/
- https://www.welivesecurity.com/es/investigaciones/eset-research-identifica-a-sandworm-como-responsable-ciberataque-a-la-red-polonia/
- https://ecosistemastartup.com/malware-wiper-ataca-red-electrica-de-polonia-claves-para-founders/
- https://www.montevideo.com.uy/Ciencia-y-Tecnologia/Red-electrica-de-Polonia-fue-atacada-por-un-malware-nunca-antes-visto-uc950899