Boletín de alerta

Boletín Nro.: 51
Fecha de publicación: 14/05/2026
Tema: Alerta 2026-51 Ataque de Supply Chain en npm orientado al robo de credenciales afecta a node-ipc
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Versiones comprometidas identificadas hasta ahora:

- node-ipc **9.1.6**
- node-ipc **9.2.3**
- node-ipc **12.0.1**

Descripción

Se ha hecho pública una nueva campaña de **supply chain attack** contra el ecosistema npm que compromete varias versiones del paquete **node-ipc**, un módulo con **más de 700.000–1.000.000 descargas semanales** según distintas fuentes de métricas públicas. En estas versiones, se ha inyectado un payload ofuscado con capacidades de **credential stealer y backdoor** tras el probable compromiso de la cuenta del mantenedor; al instalarse, el código ejecutado en postinstall recoge información sensible del entorno (tokens, claves, datos de sistema) y establece comunicación con infraestructura controlada por el atacante, permitiendo acceso remoto y movimiento lateral en entornos de desarrollo y CI/CD.

El node-ipc es un **módulo de Node.js** que facilita la comunicación entre procesos (IPC, *Inter?Process Communication*), tanto dentro de la misma máquina como, en algunos casos, entre máquinas distintas. Es ampliamente utilizado como **dependencia de infraestructura** en CLIs, herramientas de desarrollo y frameworks, porque ofrece una API sencilla para que distintos procesos Node intercambien mensajes, coordinen tareas o compartan estado sin tener que implementar sockets de bajo nivel o protocolos propios. Precisamente por ese rol “profundo” y muy reutilizado, cualquier compromiso de node-ipc puede propagarse de forma transitiva a muchos proyectos que ni siquiera lo declaran directamente en su package.json, aumentando el impacto de un Supply Chain Attack.

Dado el papel de node-ipc como dependencia transitiva en frameworks y CLIs populares, esta campaña puede impactar proyectos que nunca añadieron explícitamente node-ipc a su package.json. En contraste con el incidente de protestware de 2022 (borrado/escritura de ficheros en sistemas de Rusia/Bielorrusia), este ataque es **claramente malicioso y orientado a intrusión**, por lo que las organizaciones deben tratar

cualquier instalación de las versiones afectadas como un posible compromiso de seguridad.

Vector de compromiso

- Socket y otros investigadores señalan indicios de **compromiso del token/npm account del mantenedor** de node-ipc.
- El atacante publica versiones nuevas (9.1.6, 9.2.3, 12.0.1) con **cambios solo en el artefacto npm** (tarball), sin modificaciones visibles en el repositorio GitHub, dificultando la detección por revisiones de código.
- El paquete mantiene su descripción y metadatos normales, pasando bajo el radar de muchas herramientas que solo miran CVEs o cambios de dependencias de primer nivel.

Comportamiento del payload

Aunque el contenido concreto difiere según la versión, los patrones descritos son:

- Inclusión de un **archivo adicional ofuscado** (tamaño ~80 KB) que no está presente en versiones legítimas.
- Ejecución en postinstall o en la inicialización del módulo, lo que garantiza su ejecución en npm install/pnpm install tanto en dev como en CI/CD.
- Recolección de información de sistema:
  - usuario, hostname, rutas de proyecto;
  - tokens npm/Yarn/pnpm, posibles PATs de GitHub/GitLab encontrados en archivos de configuración;
  - variables de entorno (incluyendo credenciales cloud o secrets mal gestionados).
- Exfiltración de datos hacia dominios/infraestructura controlada por el atacante (C2 HTTP/HTTPS), con uso frecuente de ofuscación de cadenas y cifrado ligero antes de enviar.
- En algunos análisis se observa capacidad de descargar **payloads adicionales**, lo que lo convierte en un **loader/RAT** más que en un stealer simple.

En la práctica, instalar las versiones afectadas implica que la máquina de desarrollo o el runner de CI pueden considerarse **potencialmente comprometidos a nivel de usuario**.

Mitigación

Evaluar exposición

- Buscar node-ipc en todos los proyectos:
  - npm ls node-ipc
  - pnpm list node-ipc
  - yarn why node-ipc
- Revisar package-lock.json, pnpm-lock.yaml, yarn.lock para detectar uso de las versiones afectadas (9.1.6, 9.2.3, 12.0.1).
- Identificar dónde se han ejecutado installs con esas versiones, especialmente:
  - máquinas de desarrolladores;

- runners de CI/CD;
- builds de imágenes Docker.

Contención

En sistemas donde se haya detectado una versión comprometida:

- **Aislar** temporalmente la máquina de la red si es posible (sobre todo en CI/CD compartidos).
- Revisar logs de red/sistema para conexiones salientes sospechosas durante npm install y la ejecución de builds.
- Si el entorno es sensible (claves cloud, producción), considerar crear una **imagen forense** antes de limpiar.

Eliminación del paquete malicioso

- Fijar explícitamente node-ipc a una versión **segura** (por ejemplo, la última release legítima anterior al compromiso, según el aviso de Socket/npm).
- Regenerar dependencias:
  - rm -rf node_modules package-lock.json
  - npm install (o equivalente pnpm/yarn)
- En imágenes Docker, reconstruir desde cero, asegurando que el lockfile ya referencia versiones no comprometidas.

Rotación de credenciales

Asumiendo que el stealer pudo haber exfiltrado datos:

- Rotar tokens npm y PATs de GitHub/GitLab usados en esas máquinas/runners.
- Rotar credenciales de infraestructura que pudieran estar en variables de entorno (AWS_*, GCP_*, AZURE_*, etc.).
- Revisar accesos recientes en repositorios y registries en busca de actividad anómala posterior a la instalación de node-ipc malicioso.

Solución:

Es recomendado actualizar node-ipc a una versión marcada como segura por npm/Socket (por ejemplo, 9.2.x o 12.x posteriores al incidente, una vez verificados).

Evitar rangos de versión demasiado amplios en package.json (^ o ~) para dependencias de alto riesgo; usar versiones fijas y revisar cambios antes de subir de versión.

Información adicional:

- Orca Security – “Protestware in Russia NPM Package Node-ipc” https://orca.security/resources/blog/cve-2022-23812-protestware-malicious-code-node-ipc-npm-

package/
- Ekzhang – “The Node-IPC Incident” https://notes.ekzhang.com/software/node-ipc
- Snyk – Ficha de seguridad del paquete node-ipc https://security.snyk.io/package/npm/node-ipc
- SafeDep – “Compromised node-ipc on npm: Credential Stealer via Maintainer Account Takeover” https://safedep.io/malicious-node-ipc-npm-compromise
- The Hacker News – “Stealer Backdoor Found in 3 Node-IPC Versions Targeting npm Ecosystem” https://thehackernews.com/2026/05/stealer-backdoor-found-in-3-node-ipc.html
- Opsera – “How Opsera AppSec Agents Stop npm Supply Chain Attacks Before They Hit Your Build” https://www.opsera.ai/blog/how-opsera-appsec-agents-stop-npm-supply-chain-attacks-before-they-hit-your-build/