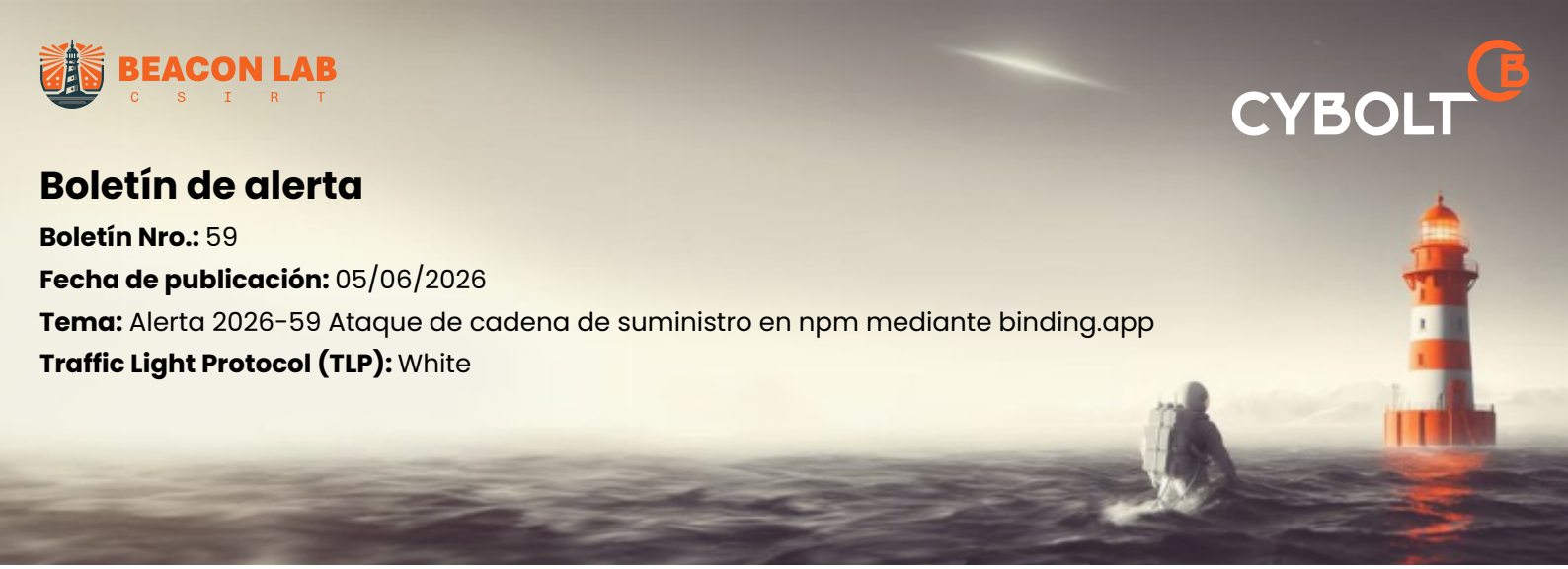

Boletín de alerta

Boletín Nro.: 59
Fecha de publicación: 05/06/2026
Tema: Alerta 2026-59 Ataque de cadena de suministro en npm mediante binding.app
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Es una campaña activa de compromiso de paquetes npm que afecta a múltiples bibliotecas JavaScript/TypeScript publicadas en el registro npm.

Entre las familias de paquetes comprometidos reportadas se encuentran:

- Autotel
- Awaitly
- Executable-stories
- Node-env-resolver
- Diversos SDK relacionados con IA
- Bibliotecas de telemetría
- Herramientas relacionadas con ESLint
- Otros paquetes mantenidos por múltiples cuentas comprometidas de npm

Descripción

Recientemente, investigadores de StepSecurity revelaron una nueva campaña de ataque contra el ecosistema npm denominada informalmente “Miasma”, un malware autorreplicante que se propaga mediante la manipulación del archivo binding.gyp, utilizado por Node.js y node-gyp para compilar módulos nativos. A diferencia de los ataques tradicionales de npm que dependen de scripts `preinstall`, `install o postinstall`, esta técnica aprovecha un mecanismo menos monitoreado por herramientas de seguridad, permitiendo la ejecución de código malicioso durante la instalación de dependencias sin modificar los scripts convencionales del archivo package.json.

La investigación indica que los atacantes insertan un archivo `binding.gyp` especialmente diseñado dentro de paquetes legítimos comprometidos. Cuando un desarrollador instala el paquete, el proceso de compilación ejecutado por `node-gyp` desencadena la carga útil maliciosa. Debido a que muchas soluciones de seguridad se enfocan principalmente en analizar scripts de instalación presentes en `package.json`, esta técnica logra evadir múltiples controles de detección existentes.

Una vez ejecutado, el malware roba credenciales y tokens asociados al ecosistema de desarrollo, incluyendo credenciales de npm, GitHub y plataformas CI/CD. Posteriormente utiliza dichos accesos para modificar y republicar otros paquetes legítimos bajo control de las víctimas, generando una propagación automática similar a un gusano (worm). Este comportamiento representa una evolución significativa respecto a campañas anteriores como Shai-Hulud y Mini Shai-Hulud, que también utilizaron el robo de credenciales para comprometer paquetes de terceros a gran escala.

El impacto potencial es elevado debido a que npm constituye uno de los repositorios de software más utilizados del mundo. Una única cuenta de mantenedor comprometida puede permitir la distribución de código malicioso a miles o millones de instalaciones descendentes, afectando estaciones de desarrollo, pipelines CI/CD, entornos cloud y aplicaciones empresariales.

Solución:

Las organizaciones que utilicen Node.js y npm deberían realizar una revisión inmediata de las dependencias instaladas recientemente, especialmente aquellas actualizadas durante los últimos días. Se recomienda identificar paquetes que incluyan archivos `binding.gyp` inesperados o modificaciones recientes no justificadas en componentes utilizados internamente.

Asimismo, es recomendable rotar de manera preventiva credenciales de npm, GitHub, GitLab, Azure DevOps y cualquier otra plataforma CI/CD que pueda haber estado accesible desde equipos de desarrollo potencialmente afectados. Los atacantes han demostrado interés específico en la exfiltración de secretos y tokens que permitan movimientos laterales dentro de la cadena de suministro de software.

Las organizaciones también deberían implementar políticas de:

- Revisión de nuevas dependencias antes de su incorporación.
- Periodos de cuarentena (cooldown period) para paquetes recién publicados.
- Firma y validación de artefactos.
- Monitorización continua de dependencias y paquetes comprometidos.
- Escaneo de estaciones de desarrollo y runners CI/CD en busca de credenciales expuestas o accesos no autorizados.

Dado que se trata de una campaña de malware y no de una vulnerabilidad específica, actualmente no existe un parche único del fabricante. La remediación depende de identificar y eliminar las versiones comprometidas de los paquetes afectados y rotar las credenciales potencialmente expuestas.

Información adicional:

- https://nvd.nist.gov/vuln/detail/cve-2026-41089
- https://www.helpnetsecurity.com/2026/06/01/windows-netlogon-rce-exploited-cve-2026-41089/
- https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs