Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE A LA CADENA DE SUMINISTRO EN NPM MÁS DE 180 PAQUETES COMPROMETIDOS

16/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

El 16 de septiembre de 2025 salió a la luz uno de los ataques a la cadena de suministro más significativos del año: la campaña “Shai-Hulud”. El ataque comprometió más de 180 paquetes NPM, entre ellos la librería popular @ctrl/tinycolor en sus versiones 4.1.1 y 4.1.2, así como proyectos mantenidos por grandes organizaciones y comunidades open-source. El objetivo de los atacantes fue robar credenciales críticas de desarrolladores y pipelines de CI/CD, logrando un vector de propagación masivo a través de la publicación de versiones maliciosas en repositorios legítimos.

El impacto va más allá de la simple distribución de paquetes contaminados: la campaña expuso tokens de NPM, secretos en GitHub Actions y llaves de servicios en la nube como AWS y GCP, lo que elevó el riesgo de compromisos completos en entornos empresariales. “Shai-Hulud” pone en evidencia cómo la identidad digital y la seguridad en los procesos de automatización son hoy el verdadero perímetro a proteger, y que cada dependencia incorporada en un pipeline representa potencialmente código con acceso directo a producción.

AKIRA RANSOMWARE INTENSIFICA ATAQUES EXPLOTANDO VULNERABILIDAD CRÍTICA EN SONICWALL

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_16_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	16/09/2025
Es día cero (0 day):	No

RESUMEN

El 16 de septiembre de 2025 se reveló un nuevo ataque a la cadena de suministro que afectó a más de 180 paquetes NPM. La campaña, bautizada como “Shai-Hulud”, se infiltró principalmente a través de la librería popular @ctrl/tinycolor en sus versiones 4.1.1 y 4.1.2, además de más de 40 proyectos adicionales mantenidos por distintos desarrolladores.
El objetivo de los atacantes fue claro: robar credenciales de desarrolladores y pipelines de CI/CD para propagar código malicioso a nuevas versiones y ampliar la superficie de ataque.

¿Cómo funcionó la INFECCIÓN?
Al instalar un paquete comprometido, se ejecutaba código diseñado para exfiltrar llaves y tokens de GitHub, AWS y GCP, entre otros servicios en la nube. Con estas credenciales, los atacantes podían:

- Publicar nuevas versiones maliciosas en proyectos legítimos.
- Infiltrarse en pipelines de integración continua (CI/CD).
- Acceder a repositorios privados y secretos corporativos.

Investigadores reportaron la detección de 34 cuentas de GitHub comprometidas, donde los atacantes creaban un repositorio público llamado *“Shai-Hulud”* para almacenar un archivo data.json con los datos robados (codificados en doble base64).

¿Quiénes se vieron afectados?

- Desarrolladores y organizaciones que instalaron las versiones alteradas durante la ventana de exposición.
- Usuarios finales, de forma indirecta, si consumieron aplicaciones compiladas con dependencias comprometidas.

Paquetes y versiones comprometidas
Entre los proyectos afectados destacan:

- @ctrl/tinycolor (4.1.1, 4.1.2)
- Paquetes de CrowdStrike (@crowdstrike/commitlint, @crowdstrike/falcon-shoelace, @crowdstrike/foundry-js, entre otros)
- Bibliotecas de @nativescript-community y @nstudio
- Proyectos de @operato, @teselagen, @things-factory, ngx-bootstrap, ngx-toastr, ng2-file-upload, entre muchos más.

La lista completa supera los 180 paquetes NPM, lo que convierte a este incidente en uno de los mayores ataques de cadena de suministro del año.

Impacto empresarial
El ataque no se limita a la distribución de malware:

- Exposición de credenciales críticas (tokens NPM, secretos de GitHub Actions, llaves en la nube).
- Posible inserción de código malicioso en aplicaciones empresariales distribuidas a clientes.
- Compromiso total de máquinas de desarrollo y CI/CD, lo que obliga a tratarlas como equipos infectados.

Medidas de contención recomendadas

1. **Eliminar o degradar** las versiones afectadas y reconstruir desde fuentes limpias.
2. **Rotar y revocar** todas las credenciales expuestas (npm tokens, llaves en la nube, GitHub PATs).
3. **Auditar registros** en busca de instalaciones sospechosas, publicaciones no autorizadas o modificaciones en workflows.
4. **Verificar repositorios** de GitHub en busca de *"Shai-Hulud"* y analizar su historial.
5. Considerar los equipos y runners comprometidos como **totalmente infectados**, realizando reinstalación o reimaging.

Lecciones aprendidas: la identidad es el nuevo perímetro

Este ataque confirma que el riesgo en la cadena de suministro ya no depende únicamente de vulnerabilidades conocidas (CVEs), sino de la confianza en identidades y automatización:

- Una cuenta comprometida puede contaminar miles de descargas semanales.
- Los atacantes ya no insertan malware solo en el código, sino que se apropian de las credenciales y tokens de CI/CD para propagarlo.

Recomendaciones estratégicas para las organizaciones

Para mitigar este tipo de incidentes, las empresas deberían:

- Implementar 2FA basado en hardware para mantenedores y pipelines.
- Usar tokens de corta duración y políticas de expiración.
- Bloquear por defecto scripts de instalación en CI/CD.
- Adoptar un periodo de enfriamiento antes de consumir nuevas versiones de librerías.
- Mantener un SBOM (Software Bill of Materials) actualizado y automatizar blocklists de dependencias maliciosas.

Conclusión

La campaña "Shai-Hulud" demuestra que cada dependencia es código con privilegios de producción en el momento en que entra al pipeline. La resiliencia ya no depende de confiar en la comunidad open-source, sino en reforzar la identidad digital y las políticas de seguridad en la cadena de suministro.
Las organizaciones deben actuar con urgencia: identidad endurecida + políticas de pipeline estrictas son la nueva base de una cadena de suministro segura.

NOTICIA COMPLETA

https://devel.group/blog/ataque-a-la-cadena-de-suministro-en-npm-mas-de-180-paquetes-comprometidos/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/