Boletín de alerta

Boletín Nro.: 74
Fecha de publicación: 10/09/2025
Tema: Alerta 2025-74 Secuestro de Paquetes de NPM populares
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- NPM de Node.js

Descripción

Se ha reportado que delincuentes comprometieron paquetes **NPM populares**, con un total de más de **2,000 millones de descargas semanales**, en lo que se clasifica como un **ataque a la cadena de suministro (Supply Chain Attack)**, denominado **Shai-Hulud**. Esta nueva cepa de malware recibe su nombre de los gusanos de arena gigantes de la saga *Dune* de Frank Herbert, ya que publica todas las credenciales robadas en un repositorio público de GitHub que incluye el nombre "Shai-Hulud".

NPM es un gestor de librerías del popular entorno de tiempo de ejecución de JavaScript llamado Node.js, el cual permite ejecutar código JavaScript en el servidor, no solo en el navegador.

Los atacantes inyectaron malware en paquetes NPM con más de 2.6 mil millones de descargas semanales después de comprometer la cuenta de un mantenedor en un ataque de phishing.

Según Aikido Security, que analizó el ataque a la cadena de suministro , los actores de la amenaza actualizaron los paquetes después de tomar el control, inyectando código malicioso que actúa como un interceptor basado en navegador en los archivos index.js, capaz de secuestrar el tráfico de la red y las API de las aplicaciones.

El malware opera inyectándose en el navegador web y monitoreando las direcciones o transferencias de billeteras de Ethereum, Bitcoin, Solana, Tron, Litecoin y Bitcoin Cash. En las respuestas de la red con transacciones de criptomonedas, reemplaza los destinos con direcciones controladas por el atacante y secuestra las transacciones antes de que se firmen. El código malicioso logra esto al enganchar funciones de JavaScript como fetch, XMLHttpRequest, y API de billetera (window.ethereum, Solana, etc.).

A continuación se listan los paquetes que se conocen fueron comprometidos durante el ataque:

- backslash@0.2.1 (0.26m descargas por semana)

- chalk-template@1.1.1 (3.9m descargas por semana)
- supports-hyperlinks@4.1.1 (19.2m descargas por semana)
- has-ansi@6.0.1 (12.1m descargas por semana)
- simple-swizzle@0.2.3 (26.26m descargas por semana)
- color-string@2.1.1 (27.48m descargas por semana)
- error-ex (47.17m descargas por semana)
- color-name@2.0.1 (191.71m descargas por semana)
- is-arrayish@0.3.3 (73.8m descargas por semana)
- slice-ansi@7.1.1 (59.8m descargas por semana)
- color-convert@3.1.1 (193.5m descargas por semana)
- wrap-ansi@9.0.1 (197.99m descargas por semana)
- ansi-regex@6.2.1 (243.64m descargas por semana)
- supports-color@10.2.1 (287.1m descargas por semana)
- strip-ansi@7.1.1 (261.17m descargas por semana)
- chalk@5.6.1 (299.99m descargas por semana)
- debug @4.4.2 (357.6m descargas por semana)
- ansi-styles@6.2.2 (371.41m descargas por semana)
- color@5.0.1

Investigadores comentan que hay varias condiciones que se devieron cumplir para que el impacto sea significativo:

- Una nueva instalación entre las 9 a. m. y las 11:30 a. m. (hora del este de EE. UU.), cuando los paquetes se vieron comprometidos
- Package-lock.json se creó durante ese tiempo
- Paquetes vulnerables en dependencias directas o transitorias

El equipo de **Socket.dev** informó que el ataque **Shai-Hulud** comprometió brevemente al menos 25 paquetes NPM administrados por **CrowdStrike**. Según CrowdStrike, tras detectar los paquetes maliciosos en el registro público de NPM, estos fueron eliminados de inmediato y se procedió a rotar las claves afectadas. **CrowdStrike aclaró que dichos paquetes no forman parte del sensor Falcon, por lo que su plataforma no se vio comprometida y los clientes permanecen protegidos.** Asi mismo, confirmaron que trabajan en conjunto con NPM y llevan a cabo una investigación exhaustiva sobre el incidente. Aún no hay información oficial desde CrowdStrike al respecto.

Mitigación:

Varios de estos paquetes ya fueron actualizados, recomendamos revisar los archivos package.json y package-lock.json para ver en que version se encuentra.

El investigador Kostas T, ha preparado una serie de comandos que le ayudará a buscar si la version de estas libraríes en la comprometida:

- Linux / MacOS

f . - \(- « *. » \) - - - '(« - »: «\^?6\.2\.2| »: «\^?4\.4\.2| »: «\^?5\.6\.1| - »: «\^?10\.2\.1| - »: «\^?7\.1\.1| - »: «\^?6\.2\.1| - »: «\^?9\.0\.1| - »: «\^?3\.1\.1| - »: «\^?2\.0\.1| - »: «\^?0\.3\.3| - »: «\^?7\.1\.1| »: «\^?5\.0\.1| - »: «\^?2\.1\.1| - »: «\^?0\.2\.3| - »: «\^?4\.1\.1| - »: «\^?6\.0\.1| - »: «\^?1\.1\.1| »: «\^?0\.2\.1»)' {} \;

- Windows

- - - . , - . |
- - '»(- »: «\^?6\.2\.2| »: «\^?4\.4\.2| »: «\^?5\.6\.1| - »: «\^?10\.2\.1| - »: «\^?7\.1\.1| - »: «\^?6\.2\.1| - »: «\^?9\.0\.1| - »: «\^?3\.1\.1| - »: «\^?2\.0\.1| - »: «\^?0\.3\.3| - »: «\^?7\.1\.1| »: «\^?5\.0\.1| - »: «\^?2\.1\.1| - »: «\^?0\.2\.3| - »: «\^?4\.1\.1| - »: «\^?6\.0\.1| - »: «\^?1\.1\.1| »: «\^?0\.2\.1»)' -

Si piensa que ha sido afectado, recomendamos realizar un reseteo de contraseñas y claves API que estuviensen almacenadas en el servidor en cuestión.

Información adicional:

- https://news.ycombinator.com/item?id=45169794
- https://www.bleepingcomputer.com/news/security/hackers-hijack-npm-packages-with-2-billion-weekly-downloads-in-supply-chain-attack/