Se reveló que una *«falla lógica»* en NPM, el administrador de paquetes predeterminado para el entorno de tiempo de ejecución de JavaScript de Node.js, que permite a los atacantes hacer pasar bibliotecas maliciosas como legítimas y engañar a los desarrolladores desprevenidos para que las instalen.

Los investigadores de la compañía de seguridad en la nube Aqua, denominaron a la amenaza de la cadena de suministro *«plantación de paquetes»*. Después de la divulgación responsable el 10 de febrero, NPM corrigió el problema subyacente el 26 de abril.

> *«Hasta hace poco, NPM permitía agregar a cualquiera como mantenedor del paquete sin notificar a estos usuarios ni obtener su consentimiento»,* dijo Yakir Kadkoda, de Aqua.

Esto significaba efectivamente que un adversario podía crear paquetes con malware y asignarlos a mantenedores populares y confiables sin su consentimiento.

La idea es agregar propietarios creíbles asociados con otras bibliotecas NPM populares al paquete envenenado controlado por el atacante con la esperanza de que al hacerlo, atraiga a los desarrolladores para que lo descarguen.

Las consecuencias de dicho ataque a la cadena de suministro son significativas por varias razones. No solo da una falsa sensación de confianza entre los desarrolladores, sino que también podría dañar la reputación de los mantenedores de paquetes legítimos.

La divulgación se produce cuando Aqua descubrió dos vulnerabilidades más en la plataforma NPM relacionadas con la autenticación de dos factores (2FA), de las que se podría abusar para facilitar los ataques de apropiación de cuentas y publicar paquetes maliciosos.

> *«El principal problema es que cualquier usuario de npm puede realizar esto y agregar otros usuarios de NPM como mantenedores de su propio paquete.*

> *Eventualmente, los desarrolladores son responsables de los paquetes de código abierto que utilizan al crear aplicaciones»,* dijo Kadkoda.