Los investigadores han detectado una vulnerabilidad de confusión de dependencias que afecta a un proyecto archivado de Apache denominado Cordova App Harness.

Los ataques de confusión de dependencias ocurren porque los gestores de paquetes revisan los repositorios públicos antes que los registros privados, lo que posibilita que un actor malicioso publique un paquete dañino con el mismo nombre en un repositorio de paquetes público.

Esto provoca que el gestor de paquetes descargue sin querer el paquete fraudulento del repositorio público en lugar del privado previsto. Si tienen éxito, pueden tener consecuencias graves, como la instalación en todos los clientes posteriores que instalen el paquete.

Un análisis de mayo de 2023 de los paquetes npm y PyPI almacenados en entornos en la nube realizado por la empresa de seguridad en la nube Orca mostró que casi el 49% de las organizaciones son vulnerables a un ataque de confusión de dependencias.

Aunque npm y otros gestores de paquetes han implementado correcciones para priorizar las versiones privadas, la compañía de seguridad informática Legit Security señaló que descubrió que el proyecto Cordova App Harness hacía referencia a una dependencia interna llamada cordova-harness-client sin especificar una ruta de archivo relativa.

La iniciativa de código abierto fue descontinuada por la Fundación Apache (ASF) a partir del 18 de abril de 2019.

Como demostró Legit Security, esto dejó abierta la posibilidad de un ataque a la cadena de suministro al cargar una versión maliciosa bajo el mismo nombre pero con un número de versión superior, lo que haría que npm obtuviera la versión falsa del registro público.

Con el paquete falso atrayendo a más de 100 descargas después de ser subido a npm, esto indica que el proyecto archivado aún está en uso, probablemente representando riesgos considerables para los usuarios.

En un escenario de ataque hipotético, un atacante podría tomar el control de la biblioteca para distribuir código malicioso que pudiera ejecutarse en el sistema objetivo al instalar el paquete.

El equipo de seguridad de Apache ha abordado el problema tomando control del paquete cordova-harness-client. Es importante señalar que se aconseja a las organizaciones crear paquetes públicos como marcadores de posición para evitar ataques de confusión de dependencias.

> *«Este descubrimiento resalta la importancia de considerar los proyectos y dependencias de terceros como posibles puntos débiles en el proceso de desarrollo*

> *de software, especialmente los proyectos de código abierto archivados que pueden no recibir actualizaciones periódicas o parches de seguridad»,* comentó el investigador de seguridad Ofek Haviv.
>
> *«Aunque pueda resultar tentador dejarlos tal como están, estos proyectos suelen tener vulnerabilidades que no reciben atención y es poco probable que se solucionen».*