Se revelaron múltiples vulnerabilidades de seguridad en los administradores de paquetes populares que, de ser explotados potencialmente, podrían ser objeto de abuso para ejecutar código arbitrario y acceder a información confidencial, incluyendo el código fuente y los tokens de acceso desde máquinas comprometidas.

Sin embargo, las vulnerabilidades requieren que los desarrolladores específicos manejen un paquete malicioso junto con uno de los administradores de paquetes afectados.

> *«Esto significa que no se puede lanzar un ataque directamente contra una máquina de desarrollador de forma remota, y requiere que se engañe al desarrollador para que cargue archivos mal formados. Pero, ¿siempre puede conocer y confiar en los propietarios de todos los paquetes que usa de Internet o de los repositorios internos de la empresa?»,* dijo Paul Gerste, investigador de SonarSource.

Los administradores de paquetes se refieren a sistemas o un conjunto de herramientas que se utilizan para automatizar la instalación, actualización y configuración de dependencias de terceros necesarias para desarrollar aplicaciones.

Aunque existen riesgos de seguridad inherentes con las bibliotecas no autorizadas que se abren camino a los repositorios de paquetes, lo que requiere que las dependencias se analicen de forma adecuada para proteger contra ataques de confusión de dependencias y errores tipográficos, el *«acto de administrar dependencias generalmente no se considera una operación potencialmente riesgosa».*

Pero las vulnerabilidades recientemente descubiertas en varios administradores de paquetes resaltan que los atacantes podrían armarlos para engañar a las víctimas para que ejecuten código malicioso. Las fallas se identificaron en los siguientes administradores de paquetes:

- Composer 1.x < 1.10.23 y 2.x < 2.1.9
- Bundler < 2.2.33
- Bower < 1.8.13

- Poetry < 1.1.9
- Yarn < 1.22.13
- pnpm < 6.15.1
- Pip (no fix)
- Pipenv (no fix)

Una de las vulnerabilidades principales es una falla de inyección de comandos en el comando de navegación de Composer, que podría abusarse para lograr la ejecución de código arbitrario al insertar una URL en un paquete malicioso ya publicado.

Si el paquete aprovecha las técnicas de error tipográfico o de confusión de dependencias, podría resultar en un escenario en el que ejecutar el comando de exploración para la biblioteca podría conducir a la recuperación de una carga útil de la siguiente etapa, que luego se podría utilizar para lanzar más ataques.

Las vulnerabilidades adicionales de inyección de argumentos y rutas de búsqueda no confiables descubiertas en Bundler, Poetry, Yarn, Composer, Pip y Pipenv, significaron que un mal actor podría obtener la ejecución del código por medio de un ejecutable git con malware o un archivo controlado por un atacante como un Gemfile que se utiliza para especificar las dependencias de los programas de Ruby.

Después de la divulgación responsable el 9 de septiembre de 2021, se publicaron correcciones para abordar los problemas en Composer, Bundler, Bower, Poetry, Yarn y Pnpm. Pero Composer, Pip, Pipenv, los tres afectados por la vulnerabilidad de la ruta de búsqueda no confiable, optaron por no solucionar el error.

> *«Los desarrolladores son un objetivo atractivo para los ciberdelincuentes porque tienen acceso a los principales activos de propiedad intelectual de una empresa: el código fuente. Comprometerlos permite a los atacantes realizar espionaje o incrustar código malicioso en los productos de una empresa. Esto incluso podría usarse para realizar ataques a la cadena de suministro»,* dijo Gerste.