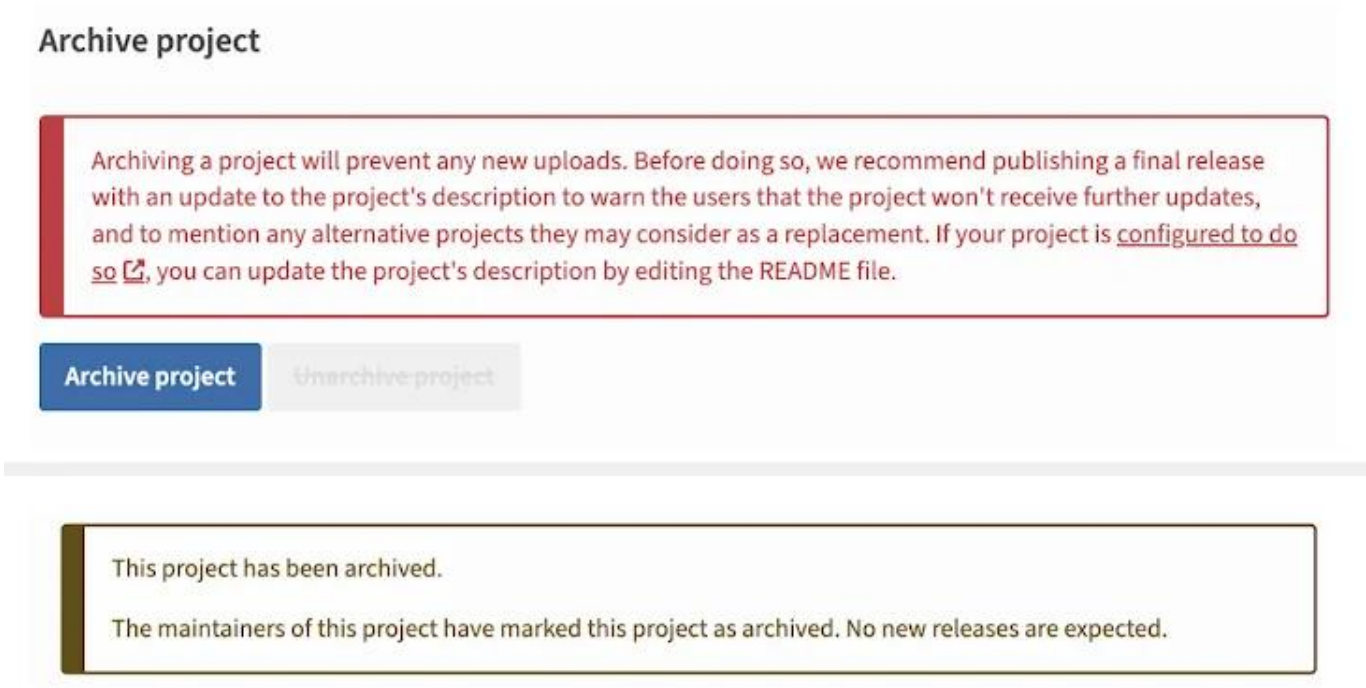
Los responsables del registro Python Package Index (PyPI) han presentado una nueva función que permite a los desarrolladores de paquetes archivar un proyecto como parte de las iniciativas para reforzar la seguridad en la cadena de suministro.

> *«Ahora los mantenedores pueden archivar un proyecto para informar a los usuarios que no se prevén más actualizaciones»,* explicó Facundo Tuesca, ingeniero sénior en Trail of Bits.

El objetivo de esta medida es dejar claro a los desarrolladores que ciertas bibliotecas de Python ya no están bajo mantenimiento activo y que no se lanzarán nuevas correcciones de seguridad ni mejoras en el producto.

Aun así, los proyectos marcados como archivados seguirán estando disponibles en PyPI, permitiendo a los usuarios su instalación sin ningún problema.

En un artículo donde detalla esta funcionalidad, Tuesca señaló que los mantenedores están evaluando la posibilidad de introducir más estados controlados por los propios desarrolladores para informar con mayor precisión a los usuarios sobre el estado de cada proyecto.



PyPI también sugiere que los desarrolladores publiquen una versión final antes de archivar un paquete, actualizando su descripción para advertir a los usuarios y proporcionando alternativas como reemplazo.

Esta novedad se suma a otra reciente actualización de PyPI: la capacidad de poner en cuarentena proyectos sospechosos, permitiendo a los administradores marcar ciertos paquetes como potencialmente peligrosos y evitar que los usuarios los instalen hasta que se realice una investigación.

En noviembre de 2024, los administradores de PyPI pusieron en cuarentena la biblioteca de Python *aiocpa* tras descubrir que una actualización reciente contenía código malicioso diseñado para robar claves privadas a través de Telegram.

Desde agosto del año pasado, aproximadamente 140 proyectos han sido puestos en cuarentena y posteriormente eliminados del registro, con una única excepción.

> *«Disponer de esta fase intermedia permite a los administradores de PyPI reaccionar con rapidez para proteger a los usuarios finales, evitando la instalación de paquetes sospechosos mientras se realiza una investigación más exhaustiva»*, explicó Mike Fiedler, administrador de PyPI.
>
> *«Dado que eliminar un proyecto en PyPI es una acción irreversible, la implementación del estado de cuarentena posibilita restaurar un paquete si se determina que la alerta fue un falso positivo, sin comprometer su historial ni metadatos.»*