Una investigación ha revelado que una gran cantidad de repositorios de software en GitHub podrían ser vulnerables a un ataque conocido como RepoJacking.

Esto incluye repositorios de organizaciones como Google, Lyft y otras más, según un informe de la firma de seguridad en la nube Aqua con sede en Massachusetts, publicado el miércoles.

Se trata de una vulnerabilidad en la cadena de suministro, también conocida como secuestro de repositorios de dependencias, que permite tomar el control de nombres de usuario o de organizaciones inactivas y publicar versiones manipuladas de los repositorios para ejecutar código malicioso.

Los investigadores Ilay Goldman y Yakir Kadkoda explicaron: *«Cuando un propietario de un repositorio cambia su nombre de usuario, se crea un enlace entre el nombre antiguo y el nuevo para aquellos que descarguen dependencias desde el antiguo repositorio. Sin embargo, es posible que cualquier persona cree el antiguo nombre de usuario y rompa este enlace».*

En otro escenario similar, esto podría ocurrir cuando la propiedad de un repositorio es transferida a otro usuario y la cuenta original es eliminada, lo que permitiría que un actor malicioso cree una cuenta con el antiguo nombre de usuario.

Aqua advierte que un actor de amenazas podría aprovechar sitios web como GHTorrent para obtener los metadatos de GitHub asociados a confirmaciones públicas y solicitudes de extracción, y así compilar una lista de repositorios únicos.

Un análisis de una muestra de 1.25 millones de repositorios durante el mes de junio de 2019 reveló que aproximadamente 36,983 repositorios eran susceptibles a RepoJacking, lo que representa una tasa de éxito del 2.95%.

Considerando que GitHub alberga más de 330 millones de repositorios, estos hallazgos sugieren que millones de repositorios podrían estar expuestos a un ataque similar.

Un ejemplo de tal repositorio es google/mathsteps, que anteriormente pertenecía a Socratic (socraticorg/mathsteps), una empresa adquirida por Google en 2018.

> *«Cuando accedes a https://github.com/socraticorg/mathsteps, eres redirigido a https://github.com/google/mathsteps, por lo que, en última instancia, el usuario obtendrá el repositorio de Google»,* explicaron los investigadores.

> *«No obstante, debido a que la organización socraticorg estaba disponible, un atacante podría crear el repositorio socraticorg/mathsteps y los usuarios que sigan las instrucciones de Google clonarán el repositorio del atacante en su lugar. Y debido a la instalación de npm, esto permitirá la ejecución de código arbitrario en los usuarios».*

Este tipo de preocupaciones no es algo nuevo. En octubre de 2022, GitHub tomó medidas para cerrar una brecha de seguridad que podría haber sido aprovechada para crear repositorios maliciosos y llevar a cabo ataques a la cadena de suministro al eludir el retiro de nombres de repositorios populares.

Para mitigar estos riesgos, se recomienda que los usuarios revisen periódicamente su código en busca de enlaces que puedan estar obteniendo recursos de repositorios externos en GitHub.

> *«Si cambias el nombre de tu organización, asegúrate de seguir siendo propietario del nombre anterior, incluso si solo es como una reserva, para evitar que los atacantes lo creen»,* señalaron los investigadores.