El servicio de alojamiento de repositorios basado en la nube GitHub compartió el viernes detalles adicionales sobre el robo de tokens OAuth de integración de GitHub el mes pasado, y dijo que el atacante pudo acceder a los datos internos de NPM y a la información de sus clientes.

> *«Usando tokens de usuario de OAuth robados que se originaron en dos integradores de terceros, Heroku y Travis CI, el atacante pudo escalar el acceso a la infraestructura de NPM»,* dijo Greg Ose, y agregó que el atacante logró obtener una serie de archivos:

- Una copia de seguridad de la base de datos de skimdb.npmjs.com que consta de datos al 7 de abril de 2021, incluido un archivo de información de usuario de 2015 y todos los manifiestos y metadatos de paquetes de NPM privados. El archivo contenía nombres de usuario, hash de contraseñas y direcciones de correo electrónico de NPM para aproximadamente 100,000 usuarios.
- Un conjunto de archivos CSV que incluyen un archivo de todos los nombres y números de versión de las versiones publicadas de todos los paquetes privados de NPM a partir del 10 de abril de 2022.
- Un *«pequeño subconjunto»* de paquetes privados de dos organizaciones.

Como consecuencia, GitHub está dando el paso de restablecer las contraseñas de los usuarios afectados. También se espera que notifique directamente a los usuarios con manifiestos de paquetes privados expuestos, metadatos, nombres y versiones de paquetes privados durante los próximos días.

La cadena de ataque, como lo detalla GitHub, implicó que el atacante abusara de los tokens de OAuth para exfiltrar repositorios privados de NPM que contenían claves de acceso de AWS, y posteriormente, aprovecharlos para obtener acceso no autorizado a la infraestructura del registro.

Hasta ahora, parece ser que el atacante no modificó ninguno de los paquetes publicados en

el registro ni se cargaron nuevas versiones de paquetes existentes en el repositorio.

Además, la compañía dijo que la investigación sobre el ataque del token OAuth reveló un problema no relacionado que involucró el descubrimiento de una *«cantidad no especificada de credenciales de usuario de texto sin formato para el registro npm que se capturaron en registros internos luego de la integración de npm en los sistemas de registro de GitHub».*

La compañía dijo que mitigó el problema antes del descubrimiento de la campaña de ataque y que eliminó los registros que contenían las credenciales de texto sin formato.

El robo de OAuth, que GitHub descubrió el 12 de abril, involucró a un actor no identificado que aprovechó los tokens de usuario de OAuth robados emitidos a dos integradores de OAuth de terceros, Heroku y Travis-CI, para descargar datos de docenas de organizaciones, incluida NPM.

La subsidiaria propiedad de Microsoft, a inicios del mes, calificó la campaña de *«altamente dirigida»* por naturaleza, y agregó que *«el atacante solo estaba enumerando organizaciones para identificar cuentas a las que apuntar selectivamente para enumerar y descargar repositorios privados».*

Desde entonces, Heroku reconoció que el robo de tokens OAuth de integración de GitHub implicó además el acceso no autorizado a una base de datos interna de clientes, lo que llevó a la empresa a restablecer todas las contraseñas de los usuarios.