El servicio de alojamiento de repositorios basado en la nube GitHub, reveló este viernes que descubrió evidencia de un adversario anónimo que aprovecha los tokens de usuario de OAuth robados para descargar datos privados de varias organizaciones sin autorización.

> *«Un atacante abusó de 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, incluyendo NPM»*, dijo Mike Hanley de GitHub.

Las aplicaciones y los servicios por lo general utilizan tokens de acceso de OAuth para autorizar el acceso a partes específicas de los datos de un usuario y comunicarse entre sí sin tener que compartir las credenciales reales. Es uno de los métodos más comunes que se utilizan para pasar la autorización de un servicio de inicio de sesión único (SSO) a otra aplicación.

A partir del 15 de abril de 2022, la lista de aplicaciones de OAuth afectadas es la siguiente:

- Tablero de HEroku (ID: 145909)
- Tablero de HEroku (ID: 628778)
- Tablero de Heroku – Clásico (ID: 363831)
- Travis CI (Número de identificación: 9216)

La compañía ha informado que los tokens de OAuth no se han obtenido a través de una violación de GitHub o sus sistemas, ya que no almacena los tokens en sus formatos originales utilizables.

Además, GitHub advirtió que el atacante puede estar analizando los contenidos del repositorio privado descargado de las entidades víctimas que utilizan estas aplicaciones OAuth de terceros para obtener secretos adicionales que después pueden aprovecharse para pasar a otras partes de su infraestructura.

La plataforma, propiedad de Microsoft, dijo que encontró evidencia temprana de la campaña

de ataque el 12 de abril cuando encontró un acceso no autorizado a su entorno de producción NPM utilizando una clave de API de AWS comprometida.

Esta clave API de AWS se obtuvo al descargar un conjunto de repositorios NPM privados no especificados utilizando el token de OAuth robado de una de las dos aplicaciones de OAuth afectadas. GitHub dijo que desde entonces revocó los tokens de acceso asociados con las aplicaciones afectadas.

> *«En este punto, evaluamos que el atacante no modificó ningún paquete ni obtuvo acceso a ningún dato o credencial de la cuenta de usuario»,* dijo la compañía.

También dijo que sigue investigando para determinar si el atacante vio o descargó paquetes privados.

GitHub también dijo que actualmente está trabajando para identificar y notificar a todos los usuarios y organizaciones víctimas conocidas que pueden verse afectadas como resultado de este incidente durante las próximas 72 horas.