El servicio de alojamiento de repositorios basado en la nube, GitHub, dijo que tomó la medida de reemplazar su clave de host RSA SSH utilizada para asegurar las operaciones de Git *«por precaución»* después de que estuvo brevemente expuesta en un repositorio público.

Dicha actividad se llevó a cabo a las 5:00 UTC del 24 de marzo de 2023, se realizó como una medida para evitar que cualquier ciberdelincuente se haga pasar por el servicio o espíe las operaciones de los usuarios a través de SSH.

> *«Esta clave no otorga acceso a la infraestructura de GitHub ni a los datos de los clientes. Este cambio solo afecta las operaciones de Git sobre SSH usando RSA»,* dijo en una publicación Mike Hanley, director de seguridad y vicepresidente sénior de ingeniería de GitHub.

El movimiento no afecta el tráfico web a GitHub.com y las operaciones de Git realizadas por medio de HTTPS. No se requiere ningún cambio para los usuarios de ECDSA o Ed25519.

La compañía propiedad de Microsoft dijo que no existe evidencia de que los atacantes hayan explotado la clave privada SSH expuesta.

Además, enfatizó que el *«problema no fue el resultado de un compromiso de ningún sistema de GitHub o información del cliente»*, culó a una *«publicación inadvertida de información privada».*

También dijo que los usuarios de GitHub Actions pueden ver ejecuciones de flujo de trabajo fallidas si están usando acciones/pago con la opción ssh-key, agregando que está en proceso de actualizar la acción en todas las etiquetas.

La divulgación se produce casi dos meses después de que GitHub revelara que hackers desconocidos lograron exfiltrar certificados de firma de código encriptado pertenecientes a algunas versiones de GitHub Desktop para aplicaciones Mac y Atom.