La plataforma de alojamiento de código GitHub, revocó las claves de autenticación SSH débiles que se generaron a través del cliente GUI de GitKraken git, debido a una vulnerabilidad en una biblioteca de terceros que aumentó la probabilidad de claves SSH duplicadas.

Como medida de precaución adicional, la compañía propiedad de Microsoft, también mencionó que está creando salvaguardas para evitar que las versiones vulnerables de GitKraken agreguen claves débiles recién generadas.

La dependencia problemática, denominada «keypair«, es una biblioteca de generación de claves SSH de código abierto que permite a los usuarios crear claves RSA para fines relacionados con la autenticación. Se ha descubierto que afecta a las versiones 7.6.x, 7.7.x y 8.0.0 de GitKraken, lanzadas entre el 12 de mayo de 2021 y el 27 de septiembre de 2021.

Pero debido a un error en el generador de números pseudoaleatorios utilizado por la biblioteca, el error resultó en la creación de una forma más débil de claves SSH públicas, que debido a su baja entropía, es decir, la medida de aleatoriedad, podría aumentar la probabilidad de duplicación de claves.

«Esto podría permitir a un atacante descifrar mensajes confidenciales u obtener acceso no autorizado a una cuenta que pertenece a la víctima», dijo Julian Gruber, mantenedor del proyecto Keypair. Desde entonces, el problema se corrigió en la versión 1.0.4 del par de claves y la versión 8.0.1 de GitKraken.

El ingeniero de Axosoft, Dan Suceava, fue reconocido por descubrir la debilidad de seguridad, mientras que el ingeniero de seguridad de GitHub, Kevin Jones, fue reconocido por identificar la causa y la ubicación del código fuente del error. Hasta ahora no existe evidencia de que la vulnerabilidad haya sido explotada en la naturaleza.

Sin embargo, se recomienda a los usuarios que revisen y *«eliminen todas las claves SSH antiguas generadas por GitKraken almacenadas de forma local y generen nuevas claves SSH utilizando GitKraken 8.0.1, o posterior, para cada uno de sus proveedores de servicios Git»,*

como GitHub, GitLab y Bitbucket.