Kraken Security Labs informó este 31 de enero que las billeteras de hardware de Trezor y sus derivados pueden ser pirateadas para extraer claves privadas. Aunque el procedimiento es muy complicado, Kraken afirma que *«requiere solo 15 minutos de acceso físico al dispositivo».*

El ataque requiere una intervención física en la billetera Trezor para extraer su chip y colocarlo en un dispositivo especial o soldando un par de conectores críticos.

El chip Trezor debe estar conectado a un *«dispositivo glitcher»* que les envíe señales en momentos específicos. Estos rompen la protección incorporada que impide que los dispositivos externos lean la memoria del chip.

Este truco permite al atacante leer los parámetros críticos de la billetera, incluyendo la semilla de la clave privada. Aunque la semilla está encriptada con una clave generada por PIN, los investigadores pudieron forzar la combinación en solo dos minutos.

La vulnerabilidad es causada por el hardware específico utilizado por Trezor, lo que significa que la compañía no puede solucionarlo fácilmente. Tendría que rediseñar completamente la billetera y recuperar todos los modelos existentes.

Debido a esto, Kraken está advirtiendo que los usuarios de Trezor y KeepKey no permitan que nadie acceda físicamente a sus billeteras.

En una respuesta coordinada publicada por Trezor, el equipo minimizó el impacto de la vulnerabilidad. La compañía argumentó que el ataque mostraría signos visibles de manipulación debido a la necesidad de abrir el dispositivo, además de mencionar que el ataque requiere un hardware extremadamente especializado para hacerlo.

La compañía sugirió que los usuarios activen la función de frase de contraseña de la billetera para protegerse de dichos ataques. La contraseña nunca se almacena en el dispositivo, ya que se agrega a la semilla para generar la clave privada sobre la marcha. Kraken también dijo que esta es una alternativa viable, aunque los investigadores se refirieron a ella como

«un poco torpe de usar en la práctica».