El exchange de criptomonedas Kraken informó que un investigador de seguridad anónimo explotó una vulnerabilidad de día cero *«extremadamente crítica»* en su plataforma para sustraer $3 millones en activos digitales y se negó a devolverlos.

Los detalles del incidente fueron compartidos por el Director de Seguridad de Kraken, Nick Percoco, en X (anteriormente Twitter), indicando que recibieron una alerta del programa Bug Bounty sobre un error que *«les permitió inflar artificialmente su saldo en nuestra plataforma»* sin dar más detalles.

La empresa comentó que identificó el problema de seguridad pocos minutos después de recibir la alerta, lo cual esencialmente permitió a un atacante *«iniciar un depósito en nuestra plataforma y recibir fondos en su cuenta sin completar totalmente el depósito.»*

Aunque Kraken subrayó que no hubo riesgo para los activos de los clientes, el problema podría haber permitido a un actor malintencionado crear activos en sus cuentas. La situación se resolvió en 47 minutos, según informaron.

También mencionaron que la falla se originó a partir de un reciente cambio en la interfaz de usuario que permite a los clientes depositar fondos y utilizarlos antes de que fueran aprobados.

Además, una investigación adicional reveló que tres cuentas, incluyendo una perteneciente al supuesto investigador de seguridad, habían explotado la vulnerabilidad con pocos días de diferencia y se habían apropiado de $3 millones.

> *«Este individuo descubrió el error en nuestro sistema de financiamiento y lo aprovechó para acreditar su cuenta con $4 en criptomonedas, esto hubiera sido suficiente para probar la falla, presentar un informe de bug bounty con nuestro equipo y recibir una recompensa muy considerable bajo los términos de nuestro programa»,* dijo Percoco.

> *«En cambio, el 'investigador de seguridad' divulgó este error a otras dos personas con las que trabaja, quienes generaron sumas mucho mayores de manera fraudulenta. Finalmente, retiraron casi $3 millones de sus cuentas de Kraken. Esto provino de las tesorerías de Kraken, no de otros activos de clientes.»*

En un giro extraño de los acontecimientos, al ser contactados por Kraken para compartir su prueba de concepto (PoC) del exploit utilizado para crear la actividad en la cadena y para arreglar la devolución de los fondos retirados, ellos exigieron que la empresa se pusiera en contacto con su equipo de desarrollo empresarial para pagar una cantidad establecida a cambio de liberar los activos.

«Esto no es hacking ético, es extorsión,» dijo Percoco, instando a las partes involucradas a devolver los fondos robados.

El nombre de la empresa no fue revelado, pero Kraken dijo que está tratando el evento de seguridad como un caso criminal y que está coordinando con agencias de la ley sobre el asunto.

> *«Como investigador de seguridad, tu licencia para 'hackear' una empresa está habilitada al seguir las simples reglas del programa de bug bounty en el que participas. Ignorar esas reglas y extorsionar a la empresa revoca tu 'licencia para hackear.' Te convierte a ti y a tu empresa en criminales»,* señaló Percoco.