En un nuevo caso de robo de criptomonedas dirigido al espacio de las finanzas descentralizadas (DeFi), los hackers robaron activos digitales por un valor de alrededor de 160 millones de dólares de la firma de comercio de criptomonedas Wintermute.

El hackeo involucró una serie de transacciones no autorizadas que transfirieron USD coin, Binance USD, Tether USD, Wrapped ETH y otras 66 criptomonedas a la billetera del atacante.

La compañía dijo que sus operaciones de finanzas descentralizadas (CeFi) y extrabursátiles (OTC) no se han visto afectadas por el incidente de seguridad. No reveló cuándo tuvo lugar el ataque.

El creador de mercado de activos digitales, que proporciona liquidez a más intercambios y plataformas criptográficas, advirtió sobre la interrupción de sus servicios en los próximos días, pero enfatizó que es *«solvente con el doble de esa cantidad en capital restante».*

> *«Estamos abiertos a tratar esto como un sombrero blanco, así que si usted es el atacante, póngase en contacto»,* dijo el fundador y directos ejecutivo de la compañía, Evgeny Gaevoy.

Los detalles que rodean el método de explotación exacto utilizado para perpetuar el ataque son desconocidos hasta ahora, aunque Gaevoy dijo que el ataque probablemente fue causado por una *«vulneración de tipo Blasfemia»* en su billetera comercial.

Wintermute reconoció además que usó Profanity, un software de generación de direcciones personalizadas de Ethereum, junto con una herramienta interna para generar direcciones con muchos ceros al frente en junio.

El proyecto de código abierto está actualmente abandonado por su mantenedor anónimo, que se hace llamar Johguse, citando *«problemas de seguridad fundamentales en la generación de claves privadas»*.

La blasfemia, por cierto, también se destacó la semana pasada después de que el agregador de intercambio descentralizado (DEX) 1inch Network, revelara una vulnerabilidad de que se podría abusar para volver a calcular las claves de la billetera privada a partir de las direcciones creadas con la utilidad.

Posteriormente, el vector de ataque fue explotado por actores maliciosos para extraer 3.3 millones de dólares de las direcciones de Ethereum creadas con Profanity el 16 de septiembre de 2022.

La violación de Wintermute es el último ataque a los protocolos DeFi, incluyendo el de Axie Infinity, Harmon Horizon Bridge, Nomad y Curve.Finance en los últimos meses. Algunos de estos robos se atribuyeron al Grupo Lazarus, respaldado por Corea del Norte.

Según un informe del obispo Fox publicado en mayo de 2022, los incidentes de seguridad que golpearon las plataformas DeFi resultaron en pérdidas por una suma de 1.8 millones de dólares solo en 2021, y los servicios experimentaron un promedio de cinco ataques por mes.

> *«En la mayoría de los casos, el ataque provino de una vulnerabilidad en los Smart Contracts o en la propia lógica del protocolo. Otro vector importante fue el compromiso de las billeteras y sus claves privadas»,* dijo la empresa.