Los investigadores de seguridad cibernética revelaron una vulnerabilidad de seguridad ya reparada en el mercado de tokens no fungibles (NFT) de Rarible, que de ser explotada con éxito, podría haber llevado a la apropiación de cuentas y robo de activos de criptomonedas.

> *«Al atraer a las víctimas para que hagan clic en un NFT malicioso, un atacante puede tomar el control total de la billetera criptográfica de la víctima para robar los fondos»,* dijeron los investigadores de Check Point, Roman Zaikin, Dikla Barda y Oved Vanunu.

Rarible es un mercado de NFT que permite a los usuarios crear, comprar y vender arte digital de NFT como fotografías, juegos y memes. Cuenta con más de 2.1 millones de usuarios activos.

> *«Todavía hay una gran brecha, en términos de seguridad, entre la infraestructura Web2 y Web3»,* dijo Vanunu, jefe de investigación de vulnerabilidades de productos en Check Point.

> *«Cualquier pequeña vulnerabilidad puede permitir que los ciberdelincuentes secuestren las billeteras criptográficas detrás de escena. Todavía estamos en un estado en el que los mercados que combinan los protocolos Web3 carecen de una perspectiva de seguridad. Las implicaciones que siguen a un hack criptográfico pueden ser extremas»*, agregó.

El modus operandi del ataque depende de que un actor malintencionado envíe un enlace a un NFT no autorizado (por ejemplo, una imagen) a posibles víctimas que, al abrir en una nueva pestaña, ejecuta código JavaScript arbitrario, lo que potencialmente permite al atacante obtener un control total sobre sus NFT enviando una solicitud setApprobalForAll a la billetera.

La API setApprovalForAll permite que un mercado transfiera artículos vendidos desde la dirección del vendedor a la dirección del comprador según el contrato inteligente implementado.

> *«Esta función es muy peligrosa por diseño porque puede permitir que cualquiera controle sus NFT si lo engañan para que lo firme»,* dijeron los investigadores.

> *«No siempre está claro para los usuarios exactamente qué permisos están otorgando al firmar una transacción. La mayoría de las veces, la víctima asume que se trata de transacciones regulares, cuando de hecho, estaban otorgando control sobre sus propios NFT».*

Al conceder la solicitud, el esquema fraudulento permite efectivamente que el adversario transfiera todos los NFT de la cuenta de la víctima, que luego el atacante puede vender en el mercado a un precio más alto.

Como medida de seguridad, se recomienda que los usuarios analicen de forma cuidadosa las solicitudes de transacciones antes de proporcionar cualquier tipo de autorización. Las aprobaciones de tokens anteriores se pueden revisar y revocar visitando la herramienta Verificador de Aprobación de Tokens de Etherscan.

> *«Los usuarios de NFT deben tener en cuenta que existen varias solicitudes de billetera; algunas de ellas se utilizan solo para conectar la billetera, pero otras pueden brindar acceso completo a sus NFT y tokens»*, dijeron los investigadores.