Se reveló una vulnerabilidad de seguridad en la versión web de la billetera Ever Surf, que de ser explotada con éxito, podría permitir que un atacante obtenga el control total de la billetera de la víctima.

> *«Al explotar la vulnerabilidad, es posible descifrar las claves privadas y las frases iniciales que se almacenan en el almacenamiento local del navegador. En otras palabras, los atacantes podrían obtener el control total de las billeteras de la víctimas»*, dijo Check Point.

Ever Surf es una billetera de criptomonedas para la cadena de bloques Everscale (antes FreeTON), que también funciona como mensajero multiplataforma y permite a los usuarios acceder a aplicaciones descentralizadas, así como enviar y recibir tokens no fungibles (NFT). Cuenta con un estimado de 669,700 cuentas en todo el mundo.

Por medio de distintos vectores de ataque, como extensiones de navegador maliciosas o enlaces de phishing, la vulnerabilidad hace posible obtener las claves cifradas de una billetera y las frases iniciales que se almacenan en el almacenamiento local del navegador, que luego pueden ser trivialmente forzadas para desviar fondos.

Debido a que la información en el almacenamiento local no está cifrada, se podría acceder a ella mediante complementos de navegador no autorizados o malware que roba información que es capaz de recopilar dichos datos de distintos navegadores web.

Después de una divulgación responsable, se lanzó una nueva aplicación de escritorio para reemplazar la versión web vulnerable, y esta última ahora está marcada obsoleta y se usa con fines de desarrollo únicamente.

> *«Tener las llaves significa control total sobre la billetera de la víctima, y por lo tanto, sobre los fondos. Cuando trabaje con criptomonedas, siempre debe tener cuidado, asegurarse de que su dispositivo esté libre de malware, no abrir enlaces*

> *sospechosos, mantener actualizado el sistema operativo y el software antivirus»,* dijo Alexander Chailytko, de Check Point.