Han salido a la luz detalles sobre una vulnerabilidad de seguridad, que ya ha sido corregida, en el casco de realidad mixta Vision Pro de Apple. Si esta vulnerabilidad se explotara con éxito, los atacantes maliciosos podrían deducir los datos ingresados en el teclado virtual del dispositivo.

El ataque, conocido como GAZEploit, ha recibido el identificador CVE-2024-40865.

> *«Es un ataque innovador que puede deducir datos biométricos relacionados con los ojos a partir de la imagen del avatar y reconstruir el texto ingresado mediante escritura controlada por la mirada»,* afirmaron un grupo de investigadores de la Universidad de Florida.
>
> *«El ataque GAZEploit aprovecha la vulnerabilidad que existe en la entrada de texto controlada por la mirada cuando los usuarios comparten un avatar virtual».*

Tras una divulgación responsable, Apple solucionó el problema en la versión 1.3 de visionOS, lanzada el 29 de julio de 2024. Describieron la falla como una que afectaba un componente llamado Presence.

«Los datos ingresados en el teclado virtual pueden inferirse a partir de Persona», explicó Apple en un comunicado de seguridad, añadiendo que resolvieron el problema *«suspendiendo Persona cuando el teclado virtual está activo».*

En resumen, los investigadores determinaron que era posible analizar los movimientos oculares (o «mirada») del avatar virtual para identificar lo que el usuario estaba escribiendo en el teclado virtual, lo que podría comprometer su privacidad.

Como consecuencia, un atacante podría potencialmente analizar avatares virtuales compartidos en videollamadas, aplicaciones de reuniones en línea o plataformas de

transmisión en vivo, y deducir de manera remota las pulsaciones de teclas. Esto podría aprovecharse para obtener información sensible, como contraseñas.

El ataque se ejecuta mediante un modelo de aprendizaje supervisado entrenado con grabaciones de Persona, el ratio de aspecto ocular (EAR), y la estimación de la mirada para distinguir entre sesiones de escritura y otras actividades en realidad virtual, como ver películas o jugar.

En el siguiente paso, las direcciones estimadas de la mirada en el teclado virtual se asignan a teclas específicas, permitiendo inferir las pulsaciones, tomando en cuenta la ubicación del teclado en el espacio virtual.

> *«Al capturar y analizar remotamente el video del avatar virtual, un atacante podría reconstruir las teclas presionadas. Es importante destacar que el ataque GAZEploit es el primero de su tipo que aprovecha la información ocular filtrada para deducir pulsaciones de teclas de manera remota»,* explicaron los investigadores.