Una vulnerabilidad de seguridad ahora parcheada en los sistemas operativos iOS y macOS de Apple, podría haber habilitado aplicaciones con acceso Bluetooth para escuchar conversaciones con Siri.

Apple dijo que *«una aplicación puede grabar audio usando un par de AirPods conectados»,* y agregó que solucionó el problema de Core Bluetooth en iOS 16.1 con derechos mejorados.

Acreditado por descubrir e informar el error en agosto de 2022, el desarrollador de aplicaciones Guilherme Rambo, quien denominó al error como SiriSpy, con el identificador CVE-2022-32946.

> *«Cualquier aplicación con acceso a Bluetooth podría grabar sus conversaciones con Siri y el audio de la función de dictado del teclado de iOS cuando usa auriculares AirPods o Beats»,* dijo Rambo en un artículo.

> *«Esto sucedería sin que la aplicación solicite permiso de acceso al micrófono y sin que la aplicación deje ningún rastro de que estaba escuchando el micrófono».*

La vulnerbilidad, según Rambo, se relaciona con un servicio llamado DoAP, que se incluye en los AirPods para soporte de Siri y Dictado, lo que permite a un atacante crear una aplicación que poría conectarse a los AirPods por medio de Bluetooth y grabar el audio en segundo plano.

Esto se ve agrabado por el hecho de que *«no hay solicitud para acceder al micrófono, y la indicación en el Centro de Control solo muestra 'Siri y Dictado', no la aplicación que estaba pasando por alto el permiso del micrófono al hablar directamente con los AirPods por medio de Bluetooth LE».*

Aunque el ataque requiere que la aplicación tenga acceso a Bluetooth, esta restricción se

puede eludir de forma trivial, ya que es poco probable que los usuarios que otorgan acceso Bluetooth a la aplicación esperen que también pueda abrir la puerta para acceder a sus conversaciones con Siri y al audio del dictado.

En macOS, sin embargo, se podría abusar del exploit para lograr una omisión total del marco de seguridad de Transparencia, Consentimiento y Control (TCC), lo que significa que cualquier aplicación puede grabar conversaciones con Siri sin solicitar ningún permiso en primer lugar.

Rambo dijo que la razón de este comportamiento se debe a la falta de verificaciones de derechos para BTLEServerAgent, el servicio daemon responsable de manejar el audio DoAP.

Un parche de software que soluciona este problema está disponible para iPhone 8 y posteriores, iPad Pro (todos los modelos), iPad Air de 3° generación y posteriores, iPad de 5° generación y posteriores, y iPad mini de 5° generación y posteriores. También se ha resuelto en todas las versiones compatibles de macOS.

La actualización de iOS 16.1, que fue lanzada el 24 de octubre de 2022, cuenta con correcciones para un total de 20 vulnerabilidades, incluyendo una falla de Kernel (CVE-2022-42827) que se reveló como explotada activamente en la naturaleza.