Una grave vulnerabilidad de seguridad en Bluetooth podría ser explotada por actores malintencionados para asumir el control de dispositivos Android, Linux, macOS e iOS.

Identificada con el código CVE-2023-45866, el problema se refiere a un caso de elusión de autenticación que permite a los atacantes conectarse a dispositivos susceptibles e introducir pulsaciones de teclas para lograr la ejecución de código como si fueran la víctima.

Marc Newlin, un investigador de seguridad, explicó: *«Varias pilas de Bluetooth tienen vulnerabilidades de elusión de autenticación que permiten a un atacante conectarse a un host detectable sin la confirmación del usuario e introducir pulsaciones de teclas»*. Newlin reveló estas debilidades a los proveedores de software en agosto de 2023.

Concretamente, el ataque engaña al dispositivo objetivo haciéndole creer que está conectado a un teclado Bluetooth al aprovechar un *«mecanismo de emparejamiento no autenticado»* definido en la especificación de Bluetooth.

La explotación exitosa de esta falla podría permitir a un adversario cercano físicamente conectarse a un dispositivo vulnerable y transmitir pulsaciones de teclas para instalar aplicaciones y ejecutar comandos arbitrarios.

Es importante destacar que este ataque no requiere hardware especializado y se puede llevar a cabo desde una computadora Linux utilizando un adaptador Bluetooth común. Se espera que se divulguen detalles técnicos adicionales sobre la falla en el futuro.

Esta vulnerabilidad afecta a una amplia gama de dispositivos que ejecutan Android (desde la versión 4.2.2, lanzada en noviembre de 2012), iOS, Linux y macOS.

Además, el error afecta a macOS e iOS cuando Bluetooth está habilitado y se ha emparejado un Magic Keyboard con el dispositivo vulnerable. También es efectivo en el Modo de Bloqueo de Apple, diseñado para proteger contra amenazas digitales sofisticadas.

En un comunicado emitido este mes, Google señaló que CVE-2023-45866 *«podría dar lugar a*

una escalada remota (próxima/adyacente) de privilegios sin necesidad de privilegios de ejecución adicionales».