Los drones que no presentan ninguna vulnerabilidad de seguridad conocida podrían ser objeto de ataques de inyección de fallos electromagnéticos (EMFI), lo que potencialmente permitiría a un agente de amenazas lograr la ejecución de código arbitrario y comprometer su funcionalidad y seguridad.

La investigación proviene de IOActive, que descubrió que es *«posible comprometer el dispositivo seleccionado mediante la inyección intencional de una falla electromagnética específica en el momento adecuado durante una actualización del firmware».*

> *«Esto permitiría a un atacante ejecutar código en el procesador principal, obteniendo acceso al sistema operativo Android que implementa la funcionalidad central del dron»,* afirmó Gabriel González, director de seguridad de hardware en el informe publicado este mes.

El estudio, llevado a cabo con el fin de evaluar el estado de seguridad actual de los Vehículos Aéreos No Tripulados (UAV), se realizó en el Mavic Pro, un dron cuadricóptero muy popular fabricado por DJI que cuenta con diversas características de seguridad, como firmware firmado y cifrado, Entorno de Ejecución Confiable (TEE) y Arranque Seguro.

Los ataques de canal lateral normalmente operan al recopilar indirectamente información sobre un sistema objetivo al explotar fugas de información no intencionadas resultantes de variaciones en el consumo de energía, emanaciones electromagnéticas y la duración de diferentes operaciones matemáticas.

El EMFI tiene como objetivo inducir una interrupción en el hardware mediante la colocación de una bobina de metal en proximidad física cercana a la CPU de control basada en Android del dron, lo que en última instancia resulta en corrupción de memoria que podría aprovecharse para lograr la ejecución de código.

> *«Esto permitiría a un atacante tener control total sobre el dispositivo, filtrar todo su*

> *contenido confidencial, habilitar el acceso ADB y potencialmente filtrar las claves de cifrado»*, mencionó González.

En cuanto a las medidas de mitigación, se recomienda que los desarrolladores de drones implementen contramedidas para el EMFI tanto a nivel de hardware como de software.

Esta no es la primera ocasión en que IOActive resalta vectores de ataque poco comunes que podrían ser empleados para dirigirse a sistemas. En junio de 2020, la compañía detalló un método innovador que permite llevar a cabo ataques a los sistemas de control industrial (ICS) utilizando escáneres de códigos de barras.

Otros análisis han mostrado configuraciones de seguridad erróneas en el protocolo de Red de Área Extensa de Largo Alcance (LoRaWAN), lo cual lo vuelve vulnerable a hackeos y ataques cibernéticos, así como vulnerabilidades en el componente de Comunicaciones de Línea de Energía (PLC) utilizado en los remolques de tractocamiones.