El Departamento de Seguridad Nacional de Estados Unidos (DHS), emitió una alerta advirtiendo a los propietarios de pequeños aviones que estén en guardia contra una vulnerabilidad que podría permitir a los atacantes piratear fácilmente el bus CAN del avión, tomando el control de los sistemas de navegación clave.

La vulnerabilidad fue descubierta por un investigador de seguridad cibernética en Rapid 7, y reside en la implementación moderna del bus CAN (Controller Area Network), un popular estándar de redes de vehículos utilizado en automóviles y pequeñas aeronaves que permite que los microcontroladores y dispositivos se comuniquen entre sí en aplicaciones sin una computadora host.

El investigador Patrick Kiley, demostró que un pirata informático con acceso físico al cableado de una pequeña aeronave podría conectar un dispositivo, o cooptar un dispositivo conectado existente, al bus CAN del avión para insertar datos falsos y comunicarlos al piloto.

> *«Las aeronaves modernas usan una red de componentes electrónicos para traducir las señales de los distintos sensores y colocar dichos datos en una red para que los instrumentos apropiados los interpreten y los muestren al piloto»,* dijo Kiley.

El hacker puede manipular los siguientes datos:

- Lecturas de telemetría del motor
- Brújula y datos de actitud
- Datos de altitud, velocidad aérea y ángulo de ataque (AoA)

> *«Los investigadores afirmaron además que un piloto que confía en las lecturas del instrumento no podría distinguir entre lecturas falsas y legítimas, lo que podría provocar la pérdida del control de la aeronave»*, dijo este martes la división cibernética del DHS.

Kiley demostró el ataque después de investigar los sistemas de aviónica (un sistema de control y navegación electrónico instalado en aeronaves) de dos fabricantes de aeronaves comerciales no identificados, especializados en aviones ligeros.

Kiley descubrió que el problema clave con el bus CAN de aviónica es que está integrado en los otros componentes del avión sin ningún firewall o autenticación, lo que significa que las conexiones no confiables por medio de un adaptador USB conectado al avión pueden enviar comandos no autorizados a sus sistemas electrónicos.

> *«En aviónica, estos sistemas proporcionan la base de los sistemas de control y sistemas de sensores y recopilan datos como altitud, velocidad del aire y los parámetros del motor, como el nivel de combustible y la presión del aceite, y luego los muestran al piloto»,* dijo el investigador.
>
> *«Los paquetes CAN tampoco tienen direcciones de destinatario ni ningún tipo de mecanismo de autenticación incorporado. Esto es lo que hace que el bus sea fácil de implementar, pero también elimina cualquier garantía de que el dispositivo emisor haya sido el autor real del mensaje»*, agregó.

Aunque el ataque suena aterrador, no es fácil obtener acceso físico (necesario para llevarlo a cabo), debido a las regulaciones actuales de la industria, sin embargo, llama mucho la atención el informe sobre la vulnerabilidad.

El investigador también señaló que el sector de aviónica está rezagado con respecto a la industria automotriz en lo que respecta al sistema de autobuses CAN.

La industria automotriz ha avanzado mucho en la implementación de seguridad, como el filtrado, lista blanca y segregación específica del bus CAN, que evita ataques físicos. Los fabricantes de aeronaves también deberían implementar dichas prácticas.

El CISA del DHS está instando a los fabricantes de aeronaves a considerar las protecciones de red alrededor del sistema de autobuses CAN y asegurarse de restringir el acceso a sus aviones lo mejor que puedan.