Google informó que está trabajando con socios del ecosistema para fortalecer la seguridad del firmware que interactúa con el sistema operativo Android.

Aunque el sistema operativo Android se ejecuta en lo que se denomina procesador de aplicaciones (AP), es solo uno de los muchos procesadores de un sistema en chip (SoC), que se ocupa de diversas tareas, como las comunicaciones celulares y el procesamiento multimedia.

> *«Asegurar la plataforma Android requiere ir más allá de los límites del procesador de aplicaciones. La estrategia de defensa en profundidad de Android también se aplica al firmware que se ejecuta en entornos bare-metal en estos microcontroladores, ya que son una parte crítica de la superficie de ataque de un dispositivo»,* dijo el equipo de Android.

La compañía dijo que el objetivo es reforzar la seguridad del software que se ejecuta en estos procesadores secundarios (firmware) y dificultar la explotación de vulnerabilidades en el aire para lograr la ejecución remota de código dentro del WiFi SoC o la banda base del celular.

Con ese fin, Google dijo que está explorando y habilitando desinfectantes basados en compiladores y activando funciones de seguridad de memoria en el firmware como medidas de mitigación de exploits.

Dadas las limitaciones de recursos asociadas con los objetivos sin sistema operativo, la idea es *«reforzar la superficie de ataque más expuesta y minimizar cualquier impacto en el rendimiento/estabilidad»*, explicó Google.

Otra área clave es el uso de lenguajes de programación seguros para la memoria como Rust, para escribir código de firmware, siguiendo sus esfuerzos para expandir su adopción en toda la plataforma.

> *«Reforzar el firmware que se ejecuta en hardware para aumentar materialmente el nivel de protección, en más superficies en Android, es una de las prioridades de la seguridad de Android»,* dijo Google.