Alrededor de unos 600,000 dispositivos de rastreo GPS para la venta en Amazon y otros grandes comerciantes en línea por 25 a 50 dólares, son vulnerables a fallas peligrosas que pueden haber expuesto las ubicaciones en tiempo real de los usuarios, según los investigadores de seguridad.

Los investigadores de seguridad de Avast descubrieron que 29 modelos de rastreadores GPS fabricados por la empresa china Shenzhen i365 para controlar a los niños pequeños, parientes mayores y mascotas, contienen una serie de vulnerabilidades de seguridad.

Además, se enviaron más de medio millón de dispositivos de seguimiento con la misma contraseña predeterminada *«123456»,* lo que brinda a los atacantes la oportunidad de acceder fácilmente a la información de seguimiento para aquellos que nunca cambiaron dicha contraseña.

Las vulnerabilidades reportadas en los dispositivos de rastreo GPS pueden permitir acceso remoto a los hackers con solo una conexión a Internet para:

- Rastrar en tiempo real las coordenadas de los dispositivos GPS
- Falsear los datos de ubicación del dispositivo para ocasionar una lectura falsa
- Acceder al micrófono de los dispositivos para espiar

La mayoría de las vulnerabilidades descubiertas se basan en el hecho de que la comunicación entre los rastreadores GPS y la nube, la nube y las aplicaciones móviles complementarias, los usuarios y la aplicación basada en la web del dispositivo, todos utilizan el protocolo HTTP de texto plano no cifrado, permitiendo a los atacantes de MiTM interceptar datos intercambiados y emitir comandos no autorizados.

> *«Todas las comunicaciones en la aplicación web pasan por HTTP. Todas las solicitudes JSON están nuevamente sin cifrar y en texto plano»*, explicaron los investigadores en un informe.

> *«Puedes hacer que el rastreador llame a un número de teléfono arbitrario y una vez conectado, puedes escuchar a través del rastreador a la otra parte sin su conocimiento. La comunicación es un protocolo basado en texto, y lo más preocupante es la falta de autorización. Todo el asunto funciona simplemente identificando el rastreador por su IMEI»*.

Además, los investigadores también descubrieron que los atacantes remotos pueden obtener coordenadas GPS en tiempo real de un dispositivo objetivo simplemente enviando un SMS al número de teléfono asociado con la tarjeta SIM que proporciona capacidades de DATA + SMS al dispositivo.

Aunque los atacantes primero necesitan saber el número de teléfono asociado y la contraseña del rastreador para llevar a cabo este ataque, los investigadores dijeron que uno puede explotar las fallas relacionadas con la nube/aplicación móvil para ordenar que el rastreador envíe un SMS a un número de teléfono arbitrario en nombre de sí mismo, lo que permite un atacante para obtener el número de teléfono del dispositivo.

Ahora, con el acceso al número de teléfono y la contraseña del dispositivo como «123456» para casi todos los dispositivos, el atacante puede usar el SMS como un vector de ataque.

El análisis de T8 Mini GPS Tracker Locator, por parte de los investigadores, también encontró que sus usuarios fueron dirigidos a un sitio web no seguro para descargar la aplicación móvil complementaria del dispositivo, exponiendo la información de los usuarios.

Los modelos afectados de dispositivos GPS incluyen T58, A9, T8S, T28, TQ, A16, A6, 3G, A18, A21, T28A, A12, A19, A20, A20S, S1, P1, FA23, A107, RomboGPS, PM01, A21P, PM02, A16X, PM03, WA3, P1-S, S6, y S9.

Aunque el fabricante de estos rastreadores GPS, Shenzhen i365 tiene su sede en China, el análisis de Avast encontró que estos rastreadores GPS son ampliamente utilizados en Estados Unidos, Europa, Australia, América del Sur y África.

Los investigadores dijeron que notificaron en privado al vendedor sobre las vulnerabilidades críticas de seguridad el 24 de junio y contactaron a la empresa varias veces, pero nunca hubo respuesta.

Martin Hron, investigador senior de Avast, dijo:

> *«Hemos realizado nuestra debida diligencia para revelar estas vulnerabilidades al fabricante, pero como no hemos tenido noticias después del plazo estándar, ahora estamos emitiendo este anuncio de servicio público a los consumidores y le recomendamos encarecidamente que deje de usar estos dispositivos»*.

Además, los investigadores aconsejaron a las personas que hicieran parte de su investigación y eligieran un dispositivo seguro de un proveedor respetado, en lugar de buscar cualquier equipo barato de una compañía desconocida en Amazon, eBay y otros mercados en línea.