



Tu ubicación online

Una nueva filtración permitió ver la ubicación en tiempo real de más de 500.000 vehículos en Estados Unidos, a través de su localizador satelital. Una vez más, la falla fue la debilidad de las claves.

Estamos llegando a un punto donde las violaciones de datos que permiten acceder a información privada se están volviendo, lamentablemente, algo normal. Ya lo veíamos hace unas semanas con el preocupante caso de *Equifax*, y antes de eso le ocurrió a *Target*, y antes a *Yahoo*, y así podemos seguir.

Hay una máxima que dice que:

"si tu información está en línea, entonces está expuesta"

Y así fue, el Centro de Seguridad de Kromtech descubrió hace unos días que cualquier persona podía acceder a la plataforma de seguimiento automotriz de 'SVR Tracking', que se dedica a la recuperación de vehículos, y así ver en directo la ubicación de más de medio millón de usuarios que decidieron contratar este servicio por cuestiones de seguridad.

SVR Tracking ofrece servicios de rastreo a vehículos por medio de un dispositivo que se coloca en un "lugar secreto" que no está accesible al conductor. Con esto, la compañía proporciona a sus clientes monitorización continua las 24 horas durante los 365 días del año.

Para que el usuario pueda dar seguimiento a la ubicación del vehículo registrado se le proporciona un número de usuario y una contraseña (que no puede ser modificada) que le permite acceder a la plataforma vía web o aplicación móvil. Asimismo, este sistema permite acceder al historial de ubicaciones y trayectos del vehículo de los últimos 120 días.

Bueno, pues Kromtech encontró el pasado 18 de septiembre 540.642 credenciales de inicio de sesión para la plataforma de SVR Tracking. Dichas credenciales se encontraban en un Amazon S3 (sitio web de almacenamiento en la nube) sin protección, por lo que fue imposible saber cuánto tiempo llevaban ahí. De hecho, tampoco se pudo saber quién fue el responsable de guardarlas, pero estaban libres para que cualquier persona accediera y las usara.

Kromtech descubrió que el problema fue que todas las contraseñas estaban codificadas con caracteres aleatorios usando el nivel de protección más débil (SHA-1), lo que hace que cualquier hacker pueda descifrarlas con cierta facilidad en poco tiempo.

Esta violación de datos también daba acceso a la plataforma de desarrollador de SVR Tracking, donde se cree que 339 registros estuvieron expuestos. En ellos se encontraban imágenes de los vehículos, bitácoras de mantenimiento y documentos que detallaban los contratos con más de 400 concesionarios de automóviles que utilizan estos servicios de localización y rastreo.



Política de escritorio limpio



Consultas, comentarios y sugerencias seginfo@estadisticaciudad.gob.ar