La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) advirtió sobre un grupo de vulnerabilidades de seguridad sin parchear en los rastreadores del Sistema de Posicionamiento Global (GPS) MiCODUS MV720, equipados en más de 1.5 millones de vehículos que podrían llevar a la interrupción remota de operaciones críticas.

> *«La explotación exitosa de estas vulnerabilidades puede permitir que un atacante remoto explote el acceso y obtenga el control del rastreador del sistema de posicionamiento global. Estas vulnerabilidades podrían afectar el acceso al suministro de combustible de un vehículo, el control del vehículo o permitir la vigilancia de la ubicación de los vehículos en los que está instalado el dispositivo»*, dijo CISA.

Disponibles a la venta por $20 dólares y fabricados por MiCODUS con sede en China, los dispositivos de seguimiento de la compañía son empleados por organizaciones importantes en 169 países que abarcan los sectores aeroespacial, energético, de ingeniería, gubernamental, de fabricación, de plantas de energía nuclear y de transporte marítimo.

Los principales países con más usuarios incluyen Chile, Australia, México, Ucrania, Rusia, Marruecos, Venezuela, Brasil, Polonia, Italia, Indonesia, Uzbekistán y Sudáfrica.

Los problemas, que se identificaron durante el curso de una auditoría de seguridad generalizada por BitSight, también podrían ser objeto de abuso potencial para rastrear a personas sin su conocimiento, desactivar vehículos e incluso plantear implicaciones de seguridad nacional a la luz del hecho de que las fuerzas armadas y las fuerzas del orden utilizan rastreadores para monitoreo en tiempo real.

> *«Un adversario de un estado-nación podría explotar las vulnerabilidades del*

> *rastreador para recopilar inteligencia sobre movimientos relacionados con el ejército, incluidas rutas de suministro, movimientos regulares de tropas y patrullas recurrentes»*, dijeron los investigadores de BitSight.

La lista de vulnerabilidades que se revelaron a MiCODUS en septiembre de 2021 son las siguientes:

- CVE-2022-2107 (puntaje CVSS: 9.8): Uso de una contraseña maestra codificada que podría permitir que un atacante no autenticado lleve a cabo ataques de adversario en el medio (AitM) y tomar el control del rastreador.
- CVE-2022-2141 (puntaje CVSS: 9.8): Esquema de autenticación roto en el servidor API que permite a un atacante controlar todo el tráfico entre el rastreador GPS y el servidor original para obtener el control.
- Sin CVE asignado (puntaje CVSS: 8.1): Uso de una contraseña predeterminada preconfigurada «123456» que permite a los atacantes acceder a cualquier rastreador GPS al azar.
- CVE-2022-2199 (puntaje CVSS: 7.5): Una vulnerabilidad de secuencias de comandos entre sitios (XSS) reflejada en el servidor web que podría conducir a la ejecución de código JavaScript arbitrario en el navegador web.
- CVE-2022-34150 (puntaje CVSS: 7.1): Una vulnerabilidad de control de acceso derivada de la referencia directa a objetos inseguros (IDOR) que podría resultar en la exposición de información confidencial.
- CVE-2022-33944 (puntaje CVSS: 6.5): Un caso de vulnerabilidad IDOR autenticada que podría aprovecharse para generar informes de Excel sobre la actividad del dispositivo.

En pocas palabras, las vulnerabilidades podrían armarse para obtener acceso a la ubicación, las rutas, los comandos de corte de combustible, así como la capacidad de desactivar varias funciones, como las alarmas.

Pero sin una solución a la vista, se recomienda a los usuarios del rastreador GPS en cuestión que tomen medidas para minimizar la exposición o, de forma alternativa, dejen de usar los

dispositivos y los deshabiliten por completo hasta que la empresa proporcione una solución.

> *«Tener un tablero centralizado para monitorear rastreadores GPS con la capacidad de habilitar o deshabilitar un vehículo, monitorear la velocidad, las rutas y aprovechar otras funciones es útil para muchas personas y organizaciones. Sin embargo, dicha funcionalidad puede presentar serios riesgos de seguridad»,* dijeron los investigadores.