Dos nuevas vulnerabilidades de seguridad fueron descubiertas en varios sistemas de carga de vehículos eléctricos (EV), que podrían explotarse para apagar estaciones de carga de forma remota e incluso, exponerlas al robo de datos y energía.

Los hallazgos, que provienen de SaiFlow, con sede en Israel, demuestran una vez más los riesgos potenciales que enfrenta la infraestructura de carga de vehículos eléctricos.

Los problemas se han identificado en la versión 1.6J del estándar Open Charge Point Protocol (OCPP) que utiliza WebSockets para la comunicación entre las estaciones de carga de vehículos eléctricos y los proveedores del sistema de gestión de estaciones de carga (CSMS). La versión actual de OCPP es 2.0.1.

> *«El estándar OCPP no define cómo un CSMS debe aceptar nuevas conexiones desde un punto de carga cuando ya hay una conexión activa»,* dijeron los investigadores de SaiFlow, Lionel Richard Saposnik y Doron Porat.

> *«Los atacantes pueden explotar la falta de una guía clara para múltiples conexiones activas para interrumpir y secuestrar la conexión entre el punto de carga y el CSMS».*

Esto también significa que un atacante cibernético podría falsificar una conexión de un cargador válido a su proveedor de CSMS cuando ya está conectado, lo que lleva a cualquiera de los dos escenarios:

- Una condición de denegación de servicio (DoS) que surge cuando el proveedor de CSMS cierra la conexión WebSocket original cuando se establece una nueva conexión.
- Robo de información que se deriva de mantener vivas las dos conexiones pero devolviendo respuesta a la *«nueva»* conexión no autorizada, lo que permite al adversario acceder a los datos personales del conductor, los detalles de la tarjeta de

crédito y las credenciales CSMS.

La falsificación es posible gracias al hecho de que los proveedores de CSMS están configurados para confiar únicamente en la identidad del punto de carga para la autenticación.

> *«Combinar el mal manejo de las nuevas conexiones con la débil autenticación OCPP y la política de identidades de los cargadores podría conducir a un gran ataque DoS distribuido (DDoS) en la red»*, dijeron los investigadores.

OCPP 2.0.1 soluciona la política de autenticación débil al requerir las credenciales del punto de carga, cerrando así la brecha. Entonces, las mitigaciones para cuando hay más de una conexión desde un solo punto de carga deberían requerir la validación de las conexiones mediante el envío de un ping o una solicitud de latido, dijo SaiFlow.

> *«Si una de las conexiones no corresponde, el CSMS debería eliminarla. Si ambas conexiones responden, el operador debería poder eliminar la conexión maliciosa directamente o mediante un módulo de seguridad cibernética integrado en CSMS»,* dijeron los investigadores.