CAI with alias0 help find flaws in MiR robots

ALIAS ROBOTICS
Robot Cybersecurity

Reto

La interfaz ROS del robot MiR aceptaba publicaciones no autenticadas en temas críticos de audio (p. ej., /mir_sound/sound_event, /data_events/ sounds) y en el servicio /mir_sound, de modo que un atacante podía activar la alarma enviando mensajes con distintos formatos sin que hubiera validación de los campos.

Solución

Se empleó CAI para generar y ejecutar un script Python (con roslibpy) que, de forma iterativa y automática, construyó múltiples cargas, probó temas y servicios en paralelo, registró los resultados y determinó qué combinaciones de campos (event, sound_id, sound_name, etc.) disparaban la alarma, ofreciendo así una herramienta reproducible de auditoría de seguridad.

Beneficio

Las pruebas de seguridad impulsadas por IA descubrieron la vulnerabilidad en solo 10 minutos y con un coste aproximado de 1 €, demostrando una forma rápida, económica y eficaz de fortalecer la protección del robot MiR frente a inyecciones de mensajes maliciosos.

Tecnología utilizada

Big Data / Data Analytics / IA

Ciberseguridad

Más información