Use Case:

Full Vehicle Penetration Test, Unauthorized Reset

Karamba Security

Background

A vehicle manufacturer requests full pen testing as part of ISO/SAE 21434 certification and the UN R155 type approval: this relates to requests for Verification and Validation cyber security controls according to threat analysis and risk assessment (TARA).

Method, Scope, and Location

1. The manufacturer has requested a full vehicle pen test with minimal budget. Grey-Box method, hybrid location, both on-site and at Karamba's remote custom labs. Among the main advantages of the hybrid location are the speed and lower costs, as many cybersecurity professionals can test simultaneously.
2. Additionally, the vehicle manufacturer has requested a Black-Box pen testing method for its vehicle.

Schedule Objectives

Karamba recommends performing the pen test as early as possible, and guides the process in carrying out and concluding the pen testing, 3-6 months before start of production (SOP). Using this approach, R&D can remediate critical findings and defects in time and re-test failures without delaying SOP.

Critical Findings

1. As part of the PT, we performed a UDS reset protocol to all ECUs and discovered that by using the OBD port, we successfully reset the braking unit while the vehicle was in motion (and not in diagnostic mode), unexpectedly stopping the vehicle.
2. As part of the Black-Box PT, we found that UDS firmware updates on the CAN could be accessed without authentication. This creates a critical vulnerability that can be exploited by altering the ECU's functionality, affecting road safety.

Impact

The impact of these findings primarily gives the OEM insight and leverage towards its Tier-1 and Tier-2 suppliers, by gaining a profound understanding of their supplied firmware and software components. Furthermore, these findings have a direct effect on SOP deadlines and avoidance of delays. Finally, ISO and UNR auditors would not certify a vehicle with these critical vulnerabilities.

Remediation

These findings send the vehicle back to R&D diagnostics to re-think and mitigate the findings. For example: Adjust and strengthen UDS authentications and limit access to reset commands, to be available solely in diagnostic mode.

Outcomes

The principal outcome of the testing and remediation is a safer vehicle delivered on time: both road-safe and cybersecure. ISO and UNR auditors certified the vehicle after reviewing all documents, findings, and remediations.