

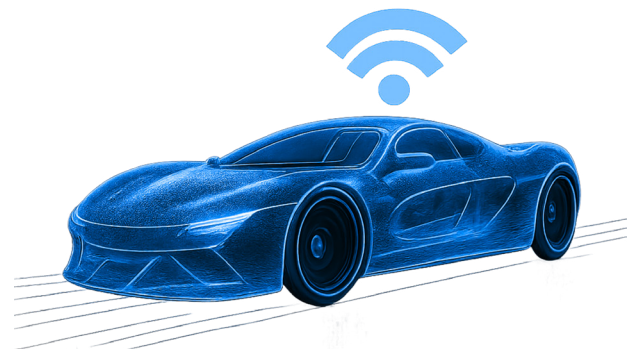
Connected Vehicle Security: Defending Automotive Systems

INDUSTRY

Automotive

OVERVIEW

Vehicles are seeing increasing connectivity through 4G/5G cellular, Bluetooth, and wireless CarPlay/Android Auto. These connected vehicle systems present soft targets that could lead to memory corruption attacks that can be used to gain initial remote access into the vehicle. By implementing RunSafe's advanced security measures, OEMs and Tier 1 vendors can comply with automotive safety standards like ISO 21434, ISO 26262, SAE J3061, and UNECE WP.29.



CHALLENGE

Connected vehicles are a part of the Internet of Things (IoT) and interact and share real-time data about the vehicle and its passengers/cargo with the world around them.

- **Telematic systems** connect the smart vehicle to the OEM's cloud for navigation and diagnostic information.
- **Infotainment systems** connect the driver/passenger with personal navigation or entertainment services.
- **V2X** describes a variety of scenarios, like **Vehicle to Infrastructure (V2I)** that connects vehicles to Smart Cities, **Vehicle to Home (V2H)** that connects BEVs to home for energy transfer, and **Vehicle to Network (V2N)** that connects vehicles to cellular and satellite networks.

A memory corruption attack through any of these vehicle connectivity systems can lead to remote access, allowing attackers to remotely start and stop vehicles or even control steering, braking, and acceleration.



SOLUTION

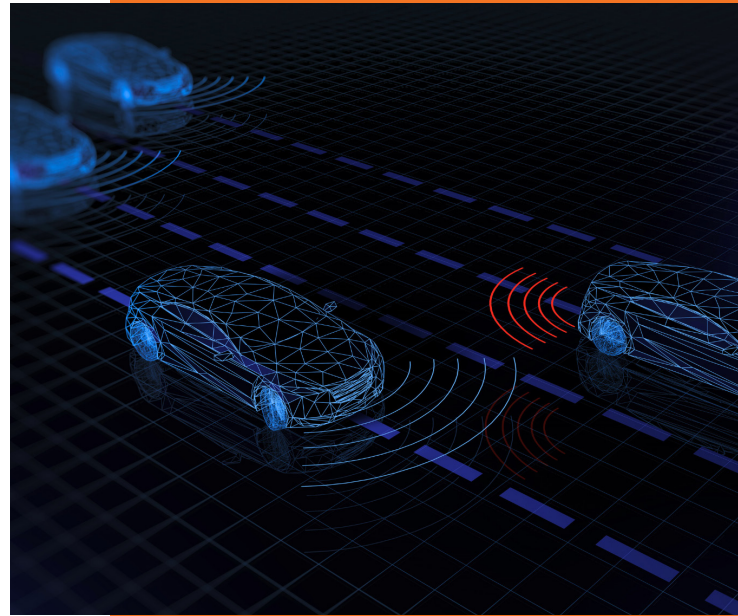
RunSafe offers a cybersecurity solution designed to keep connected automotive systems secure against known and unknown vulnerabilities.

Key features of RunSafe's solution include:

- **Automated build-time SBOM generation, including for C/C++:** RunSafe supports compliance with SBOM and software supply chain standards with build-time SBOM generation and automated vulnerability identification to reduce your risk.
- **Automated mitigation and code protection:** By using patented runtime protection technology to cyberharden vehicle components, RunSafe reduces opportunities for attackers to exploit memory safety vulnerabilities and take control of critical systems. RunSafe's solution identifies and mitigates risks before they can impact vehicle safety and operation.
- **Seamless integration:** RunSafe's cybersecurity measures are easily integrated into your existing CI/CD pipeline and align with existing automotive safety standards (such as ISO/SAE 21434 and ISO 26262), improving compliance and enhancing the overall safety of vehicle systems.
- **Futureproof from zero days:** By protecting against known and unknown vulnerabilities and denying the building blocks of zero days, RunSafe prevents future attacks by eliminating the entire class of memory safety vulnerabilities.

KEY FEATURES

- Build-time SBOM generation, including for C/C++
- Automated mitigation and runtime code protection
- Seamless integration
- Futureproofing from memory-based zero days



Examples


Jeep Cherokee Hack (2015): A vulnerability in the Uconnect infotainment module, exploited via cellular network, led to remote control of steering and brakes.

Example Vulnerability: CVE-2025-2082

CVE-2025-2082 is a critical integer overflow in the Tesla Model 3's Vehicle Control System Electronic Controller (VCSEC), exploitable via the Tire Pressure Monitoring System. Attackers within Bluetooth or Wi-Fi range could execute arbitrary code on the VCSEC and send unauthorized CAN bus commands, potentially affecting core functions like braking or acceleration.



 RunSafeSecurity.com

 571.441.5076

 Sales@RunSafeSecurity.com

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals.