NETRISE

EV Manufacturing - Use Cases

For Device Manufacturers

A Complex Problem

Electric Vehicles (EV) are complex systems made up of parts sourced from a variety of manufacturers, with many of these parts requiring firmware to operate. Each piece of firmware can include open-source and proprietary components from both the parts and EV manufacturers. According to Ford CEO Jim Farley, auto manufacturers utilize components from “150 different suppliers who don’t talk to each other.” The criticality of firmware in intra-vehicular communication and over-the-air updates creates further pressure on the security of these critical components.

As EVs use more smart components and become increasingly reliant on their associated firmware, the responsibility falls on auto manufacturers to identify and address the attack vectors of their vehicles. In order to do this effectively and efficiently, they need to fully understand what software and firmware exists in these vehicles and properly enumerate the components, vulnerabilities, and configuration issues.

The NetRise Platform use cases below are geared for the needs of different teams at EV manufacturers. Users benefiting from these use cases include:

- **Development teams**, who need to review vulnerabilities and plan the appropriate remediation activities.
- **Product management teams**, now able to prepare documentation and generate Software Bill of Materials (SBOMs) as required by fleet owners and governmental bodies.
- **Product Security and Incident Response Teams (PSIRT)**, who benefit from the ability to search for individual firmware images and identify where a given vulnerability is across their entire library of firmware.

> The NetRise Platform is purpose-built for firmware component identification and utilizes many technologies, from deep binary analysis, to open source package analysis, to function hashing, all the way to novel data science and machine learning approaches. This combination of breadth and depth in methodology provides the most comprehensive inventory of components possible, and therefore the most accurate SBOMs, including insights into the complex relationships between components. Since the vulnerability information derives from the list of components, having the most accurate inventory of components is a pivotal factor when attempting to provide the most complete list of vulnerabilities for a device.

Key Use Cases

01 | Development

NetRise saves product security teams time by identifying vulnerabilities, misconfigurations, and other sources of risk across all products, and enriching vulnerability data to provide better context for prioritization. Using exploit availability, threat actor correlation, and vulnerability enrichment data provided by the NetRise Platform, security teams can focus on the vulnerabilities that pose the most tangible risk, including those that may not be categorized as a High or Critical risk according to CVSS and those identified in CISA's Known Exploited Vulnerabilities (KEV) Catalog. NetRise enables its customers to focus on the risks that will have the greatest impact in reducing the attack surface, and therefore be more efficient and effective while enhancing security.

02 | Product Management

The NetRise Platform allows product teams to easily generate more accurate product documentation with the most accurate SBOMs derived from the actual binary version of the various firmware running on the EV. This critical documentation will prove essential to procurement processes as large fleets of EVs are ordered by the likes of the US Postal Service and the military.

03 | Product Security Incident Response Team (PSIRT)

Identifying and assessing security issues frequently discovered in software as part of a manufacturer's custom code or within open-source code grants the ability to investigate, validate, and if necessary, reduce the time needed to resolve the issue prior to public disclosure. Additionally, manufacturers can instantly search the organization's entire library of firmware to confirm which devices contain vulnerable code and which products are clean. In the event of an attack, the PSIRT has immediate access to all of the firmware for all of the various components within the vehicle, enabling rapid analysis and remediation — which could ordinarily take weeks or more.

04 | Firmware Library Searches

From the moment a new issue hits the news, as we saw with Log4j, the PSIRT scrambles to determine if it exists anywhere in their product base. With the NetRise Platform, the PSIRT can search their library of firmware and instantly see which products contain the new vulnerabilities and start the communication and remediation processes.

05 | Resources

All of the resources involved in the use cases above are highly-skilled and in high demand. The ability to save the time of these valuable individuals has a real benefit in minimizing costs and reducing delays in product release schedules. Minimizing delays can have a significant impact on revenues and profits, as well as safety, security, and compliance efforts for connected vehicles.

Ready for a Demo?

netrise.io | sales@netrise.io

Copyright © 2023 NetRise, Inc.