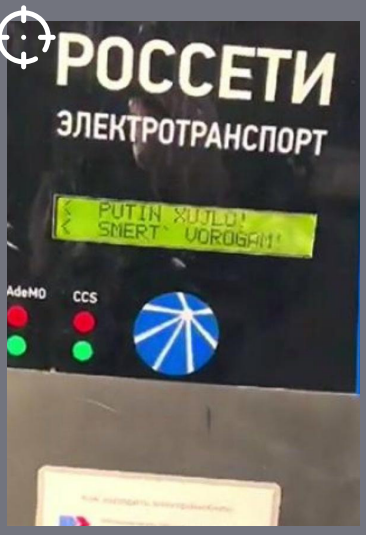
NETRISE

EV Charging System - Use Cases

For Device Manufacturers

A Complex Problem

Electric Vehicle (EV) charging stations are complex systems with many components sourced from a variety of manufacturers. Beyond the AC-to-DC converter there will be touch screens, credit card readers, environmental monitoring equipment, just to name a few of the items housed within the enclosure. Each of these components can be monitored and adjusted remotely. The complexity and remote management open these charging stations to a variety of attacks from sophisticated attackers.



Russian Systems Hacked

EV charging station hacks are not just theoretical or lab demonstrations. In February 2022 a Russian network of charging stations were taken offline and displayed pro-Ukrainian messages. Attacks could target the system's user database, credit card information and potentially cause physical damage to the stations. In addition it might be possible to jump from the station to the vehicle plugged in and impact that vehicle.

With all of these risks it is incumbent upon the manufacturers of these systems as well as the owner/operators to fully understand what software and firmware exists in these devices and fully enumerate the components, vulnerabilities, and configuration issues.

The NetRise Platform is a cloud-based SaaS solution that analyzes firmware from the binary in a fully automated fashion. It identifies the components within the firmware and can generate a Software Bill of Materials (SBOM). It provides a comprehensive list of vulnerabilities for the firmware analyzed. NetRise's vulnerability enrichment allows product security teams to prioritize vulnerabilities based on threat intelligence, exploit availability, and other criteria

Key Use Cases

01 | Development Team

Most software development shops spend significant time scoping, tracking, and remediating software issues including security vulnerabilities. NetRise saves time by identifying vulnerabilities across all products, 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. NetRise enables its customers to focus on the vulnerabilities that will have the greatest impact in reducing the attack surface, and therefore be more efficient and effective while enhancing the security of a device..

02 | Product Management and Marketing

The Product Management and Marketing teams will benefit from the greater availability and more detailed information for the products they support. Product documentation, including hardening guides, will be easier to generate and more accurate.

03 | Product Security Incident Response Team (PSIRT)

The PSIRT investigates reported vulnerabilities that may exist within one or more of the Company's products. Security issues are frequently discovered in software which can be part of a manufacturer's custom code or it can be within open-source code that the manufacturer utilized during their development process. Vulnerabilities in open-source components are frequently publicly announced with no advance notice. In either case an important aspect of the response process is to determine where the impacted component exists. The ability to instantly search the organization's entire library of firmware to confirm which devices contain the vulnerable code and which products are clean is an important step in the response process. Should an attack be successful, the PSIRT team will need immediate access to query all of the firmware for all of the various components within the EV charging station. Without immediate access analysis and remediation activities to bring the charging stations back online could stretch out to be weeks.

04 | Firmware Library Searches

From time-to-time a new broad-based vulnerability (e.g. Log4j) is announced. From the moment that new issue hits the news 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 instantaneously see which products contain that new vulnerabilities and start the communications and remediation processes.

05 | Resources

All of the staff involved in the use cases above are highly-skilled and in high demand. The ability to save the time of these individuals has a real benefit in minimizing costs throughout the product lifecycle. The ability to minimize delays can have a significant impact in revenues and profits.

Ready for a Demo?

netrise.io | sales@netrise.io