FirmwareIQ combines the depth and precision of expert binary analysis with the speed and efficiency of cloud computing to provide users with the analytic data they need to identify and eliminate security vulnerabilities in their Linux, Android and Docker® software packages.

Designed for software developers, security analysts and buyers of firmware-based systems, the FirmwareIQ analytic engine outputs a comprehensive security analysis of the target software. The interactive report can be navigated, organized and sorted to provide the most relevant data for the user’s security needs.

features

- Software Components (CVEs)
- Keys and Certificates
- Passwords
- Wireless Configuration
- Web Servers/Web Apps
- Permissions
- Firewalls
- User Account Settings
- Scripting
- Remote Access Settings
- Kernel Configuration

www.harborlabs.com
fast and comprehensive analysis
FirmwareIQ performs thousands of individual inspections to provide a comprehensive cybersecurity profile of the target software. In just minutes, FirmwareIQ generates a report that would take hours, even days for a team of experts to produce manually.

standardized, portable scoring
Rather than provide a subjective, proprietary security score, FirmwareIQ generates a composite Common Vulnerability Scoring System (CVSS) score for the target software, as well as CVSS scores for each individual vulnerability and security category. As a global standard for calculating vulnerability metrics, CVSS scores can be applied in multiple cybersecurity scenarios outside of FirmwareIQ.

precise file identification
Harbor Labs’ patent-pending system for extracting and identifying file types produces high fidelity recreations of the target file system, regardless of naming conventions or file constructs. As a result, vulnerabilities are not overlooked or incorrectly flagged due to an unidentified or misidentified file type.

no source code required
FirmwareIQ does not require source code for its analysis, instead performing automated analysis on the binary package only. The risk of exposing valuable IP in source code is removed without compromising the quality or fidelity of the analytic output.

elimination of false positives
With many automated analysis tools, the process of reviewing analytic output to distinguishing false positives from genuine vulnerabilities can be a cumbersome and time-consuming process. FirmwareIQ eliminates false positives in order to rapidly isolate and remedy the most high-priority vulnerabilities.

www.harborlabs.com