![BlackBerry QNX]

BLACKBERRY JARVIS 2.0

Software Composition Analysis and Security Testing for Embedded Systems

PRODUCT BRIEF

UNCOVER SOFTWARE VULNERABILITIES ACROSS YOUR COMPLEX SUPPLY CHAIN

Understanding the software composition and vulnerability exposure of embedded systems can be challenging. This is particularly true in industries like automotive, aerospace and defense, and medical equipment where the challenges of managing material from complex supply chains are compounded by stringent regulatory requirements.

BlackBerry® Jarvis® 2.0 is a software composition analysis and static application security testing solution that is designed to analyze binaries within complex embedded systems. It lets you identify security vulnerabilities in products that have software from multiple sources, without the need for source code. It's a powerful tool that provides you insights into your binaries and helps you catch potential security issues with the click.
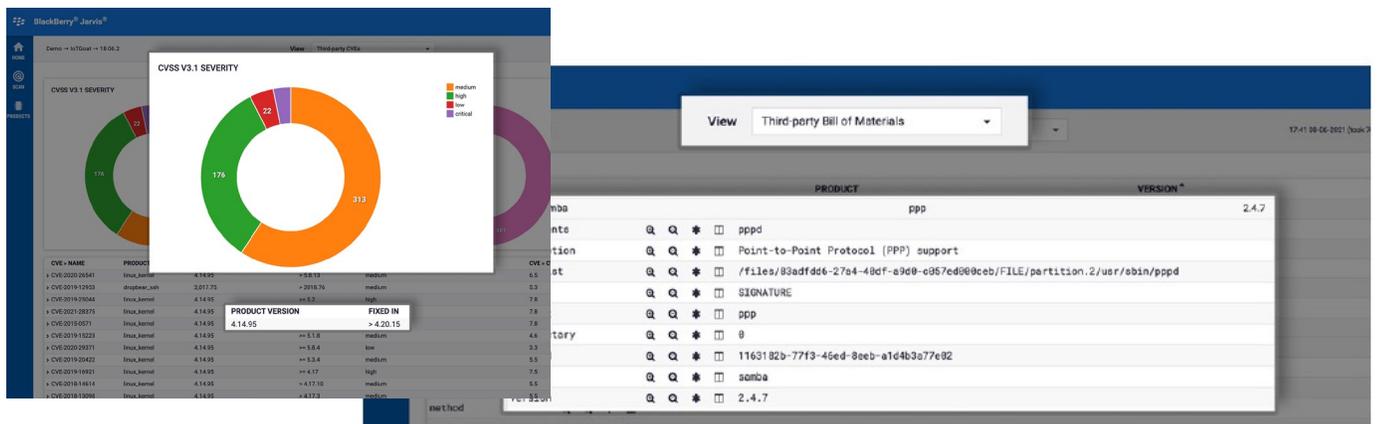
Figure 1:

BlackBerry Jarvis reveals a rich set of details for the files contained in your binary package.

SIMPLIFY REGULATORY COMPLIANCE

While regulations for embedded systems once focused on safety, security standards are emerging in response to governments and other regulating bodies demanding that manufacturers become more accountable for the security of their products.

For example, the U.S. government's Executive Order on Improving the Nation's Cybersecurity (14028) requires its vendors to provide a software bill of materials (SBOM) and demonstrate cybersecurity management measures. This regulation impacts any vendor, supplier, or provider of technology solutions to the U.S. government, particularly in areas such as defense and critical infrastructure.

As another example, WP.29, the United Nations Economic Commission for Europe's (UNECE's)

Sustainable Transport Division working party, has set out an international automotive cybersecurity regulation to establish performance and audit requirements for cybersecurity and software update management for new passenger vehicles sold in the European Union and dozens of other countries. The WP.29 regulations require that OEMs demonstrate that they are managing their cybersecurity risks. So being able to provide an SBOM will help organizations comply with the regulation.

BlackBerry Jarvis 2.0 enables you to generate a comprehensive SBOM in the Software Package Data Exchange® (SPDX®) report standard, one of the leading standards to support Executive Order 14028. This ability to efficiently produce a standards-compliant SBOM is critical for the cybersecurity management required by emerging regulations.

Figure 2:

BlackBerry Jarvis 2.0 provides a comprehensive SBOM in the Software Package Data Exchange® (SPDX®) report standard.

IDENTIFY SECURITY VULNERABILITIES

Security vulnerabilities are software defects that hackers can exploit to attack a system. Companies with sound security practices are vigilant in tracking, managing and remediating vulnerabilities. However, if you are integrating software of unknown provenance (SOUP) and have no access to source code, you may be unknowingly including security vulnerabilities in your product. BlackBerry Jarvis is unique in its ability to help you accurately identify vulnerabilities in these scenarios. Designed for embedded applications, it supports an extensive list of file formats and hardware architectures used in embedded devices.

To accurately uncover vulnerabilities in open-source components, you need to identify both the component and its version accurately. Without identifying the version, it is easy to miss a vulnerability or produce false positive results. This type of inaccuracy can be costly to you and your suppliers. BlackBerry Jarvis 2.0 excels in accurately detecting vulnerabilities thanks to its strong ability to accurately identify OSS versions.

Beyond identifying Common Vulnerabilities and Exposures (CVEs) in open-source components, BlackBerry Jarvis 2.0 can uncover a rich set of security data to help security professionals gain an in-depth view of the software's security posture and find ways to harden it. The tool discovers, collects, analyzes and presents this data with a series of interactive dashboards, each rendering a specific security perspective, such as compiler defense, information leakage and insecure API to name a few examples. To push even further, BlackBerry Jarvis 2.0 combines all this security intelligence and produces a list of Cautions that highlights the security gaps in the binaries, and on what remediation actions can be taken – all without requiring access to source code.

Figure 3:

BlackBerry Jarvis can identify a wide variety of hardware and file types used in embedded systems. Its accurate version identification is the key to reliably uncovering vulnerabilities.

EXPERT ANALYSIS WITH BLACKBERRY SECURITY SERVICES

When your needs are more complex, you can rely on BlackBerry® cybersecurity expertise to provide further insights into your software exposure, or to help you improve your overall security posture. Our embedded security professionals are ready to help you dive deeper into the results of your software analysis and identify areas that need hardening and remediation. We can also help your organization meet cybersecurity regulations from both process and product perspectives.

Learn more about our Security Services.

"

"BlackBerry Jarvis addresses the software cybersecurity needs of the automotive industry. In our independent study, Jarvis delivered excellent efficiencies in time-to-market, significantly reducing the time to security-assess code from thirty days to seven minutes."

Dr. Ralf Speth, Former CEO, Jaguar Land Rover

PRODUCT FEATURES

BlackBerry Jarvis helps you better understand the quality and composition of your software, enabling you to catalogue your software components and monitor your risk profile.

Intuitive Dashboards	Open-Source Software (OSS) Detection
Quickly identify areas of risk with CVSS scoring, allowing organizations to prioritize corrective actions	Determine the open- source software Bill of Materials (BOM) to assess associated risk and compliance
Common Vulnerabilities and Exposures (CVE)	**Software Bill of Materials (SBOM)**
Determine the public CVE associated with the OSS BOM using current NIST data	Uncover potential risks hidden in the binary package of your complex product. The SBOM lets you get an accurate view your product's SBOM without having to rely on material provided by suppliers

TECHNICAL SPECIFICATIONS

BlackBerry Jarvis was designed for embedded software and covers a wide range of software, formats, operating systems, and hardware that can be combined to create binary packages.

Archive Formats	Hardware Architectures	OS Platforms	Programming Languages
• Various forms of compressed formats including ZIP, GZIP, TAR, RAR, AR • Virtual machine binary formats including VMDK, QCOW2 and DOS partitions • Linux/Unix package file formats including RPM, DEB, JAR and APK • Android package formats including Android Sparse Image, Boot Image and SDAT • Archives for various file systems including FAT, EXT4, QNX FS, JFFS2, SQUASHFS and CDROM	• ARM: v5, v6, v7, v8-A32 and 64 bits • Intel x86 32 and 64 bits • Power 32 bit, VLE • Infineon TriCore • Renesas V850, RH850, RL78 • MIPS 32 bit • Sparc 32 bit • AVR32	• Linux: ELF and SO • Android: ELF, SO, APK • QNX 6 and 7: ELF and SO • VxWorks 5 and 6 • Classic AutoSAR • Dalvik: ART • Oracle Java: JAR, CLASS • Media: EXIF data, such as geo-tagging	• C • C++ • Java • Assembly

BlackBerry | QNX

About BlackBerry QNX: BlackBerry QNX is a trusted supplier of safe and secure operating systems, hypervisors, frameworks and development tools, and provides expert support and services for building the world's most critical embedded systems. The company's technology is trusted in more than 195 million vehicles and is deployed in embedded systems around the world, across a range of industries including automotive, medical devices, industrial controls, transportation, heavy machinery and robotics. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

BlackBerry® QNX® software and development tools are standards-based and enable companies to adopt a scalable software platform strategy across product lines and business units. The BlackBerry QNX software portfolio, including safety pre-certified products, is purpose-built for embedded systems and scales from single-purpose devices to highly complex systems of mixed criticality. Because we are successful only when you are, you can rely on our support and professional services teams to provide the expertise you need, when you need it—throughout the entire product development life cycle.