BlackBerry | QNX

BLACKBERRY JARVIS 2.0

Software Composition Analysis for Embedded Systems

PRODUCT BRIEF

UNCOVER SOFTWARE VULNERABILITIES ACROSS YOUR COMPLEX SUPPLY CHAIN

It's challenging to fully understand your software's composition and vulnerabilities. This is particularly true in industries like aerospace and defense, automotive and medical equipment, in which the complexities of managing material from supply chains are compounded by stringent regulatory requirements.

BlackBerry® Jarvis® 2.0 analyzes binaries within complex embedded systems, allowing you to identify security vulnerabilities in products with software of various origins—without the need for source code. It's a powerful tool that provides you insights into your binaries and can help you catch potential security issues with a single click.

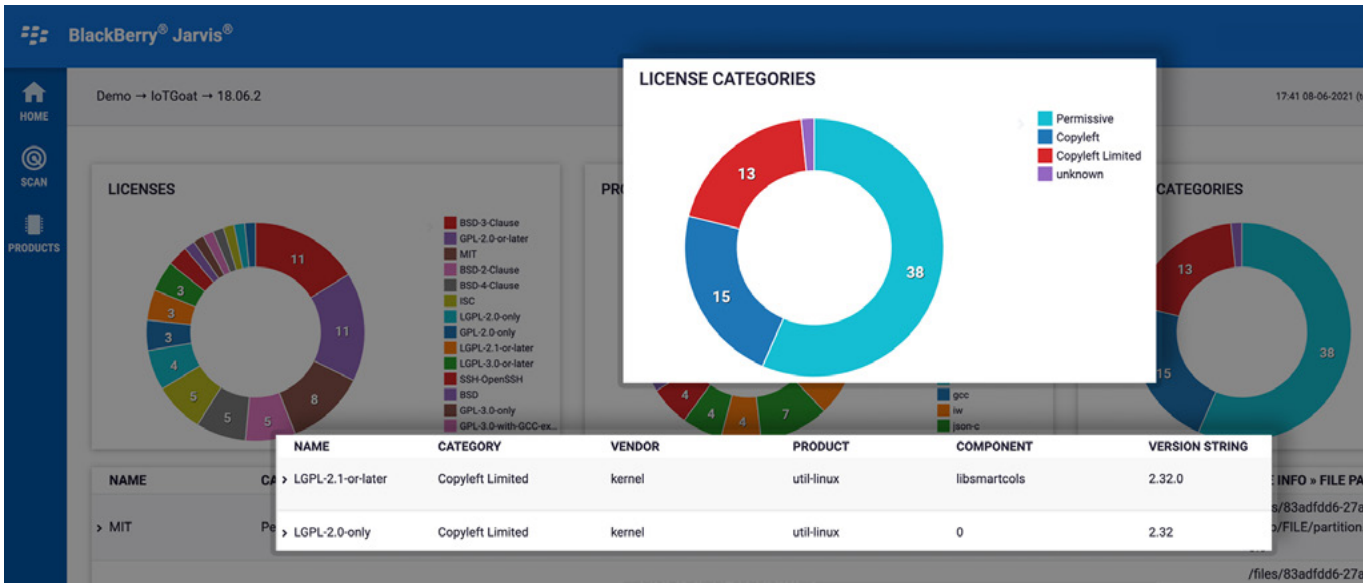

Figure 1: BlackBerry Jarvis reveals all the files used to create your binary package.

SIMPLIFY REGULATORY COMPLIANCE

While embedded systems regulations used to focus on safety, security standards are beginning to make manufacturers more accountable for the security of their products.

For example, the U.S. government's Executive Order on Improving the Nation's Cybersecurity requires its vendors to provide software bills of materials (SBOMs) and demonstrate cybersecurity management. This regulation impacts all vendors, suppliers and providers of technology solutions to the U.S. government, particularly in those working in 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 established an international automotive cybersecurity regulation that includes performance and audit requirements for cybersecurity and software update management for new passenger vehicles sold in the European Union and many other countries. The WP.29 regulations require that OEMs demonstrate that they are managing cybersecurity risks.

BlackBerry Jarvis enables you to uncover and analyze the software composition of your products by producing an SBOM—without having to access source code and in a fraction of the time it takes to complete these tasks manually. This ability to efficiently produce an accurate SBOM is the foundation of the cybersecurity management required by emerging regulations.

DISCOVER WHAT'S HIDDEN IN YOUR BINARIES

Do you know what software is running on your production systems? An SBOM can help you identify critical information about software components. Just as a savvy grocery shopper scrutinizes the nutrition labels on food packages, an experienced systems integrator can read an SBOM to examine binary files and detect issues that may have implications for intellectual property disputes, security risks and overall quality.

BlackBerry Jarvis lets you uncover potential risks hidden in the binary package of your products, enabling you to view your products' SBOMs without having to rely on information provided by your suppliers. In turn, you'll be able to assess risk and plan appropriate actions to mitigate risk.

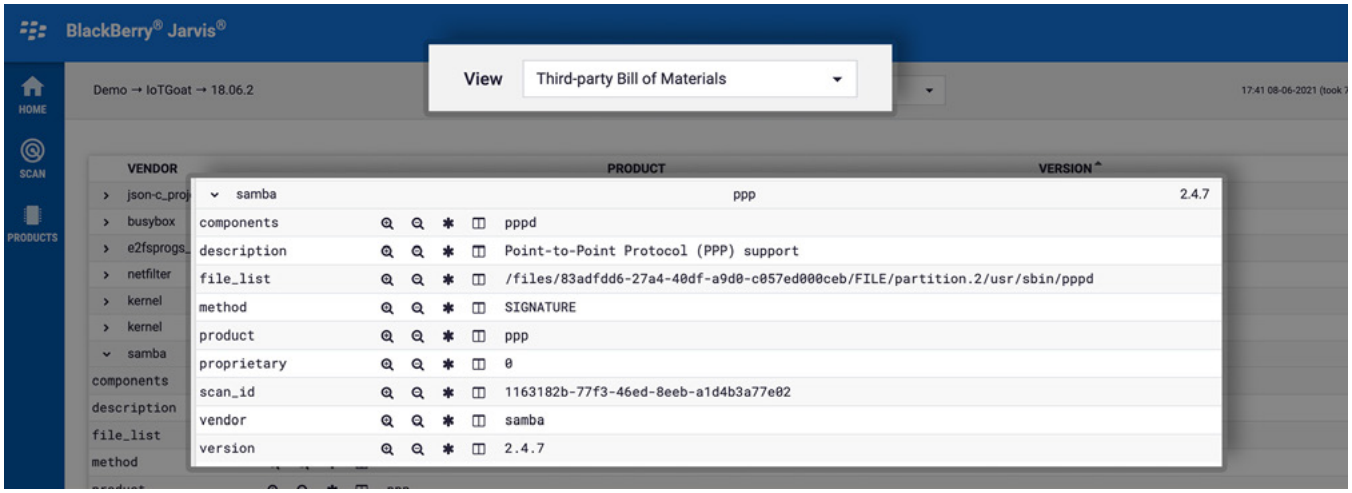

Figure 2: BlackBerry Jarvis 2.0 helps you view and manage your software bill of materials.

IDENTIFY ALL YOUR CODE VULNERABILITIES

Security vulnerabilities are software defects that bad actors 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 introducing security vulnerabilities into your product. BlackBerry Jarvis is unique in its ability to help you accurately identify vulnerabilities in SOUP. Designed for embedded applications, it supports an extensive list of file formats and hardware architectures used in embedded devices.

To accurately uncover vulnerabilities, you need to identify open-source components and their versions. Without identifying versions, it is easy to miss vulnerabilities or produce false positives. This type of inaccuracy can be costly to you and your suppliers. BlackBerry Jarvis excels in accurately detecting common vulnerability exposures (CVEs) with its ability to identify software versions, and when fixes were made.

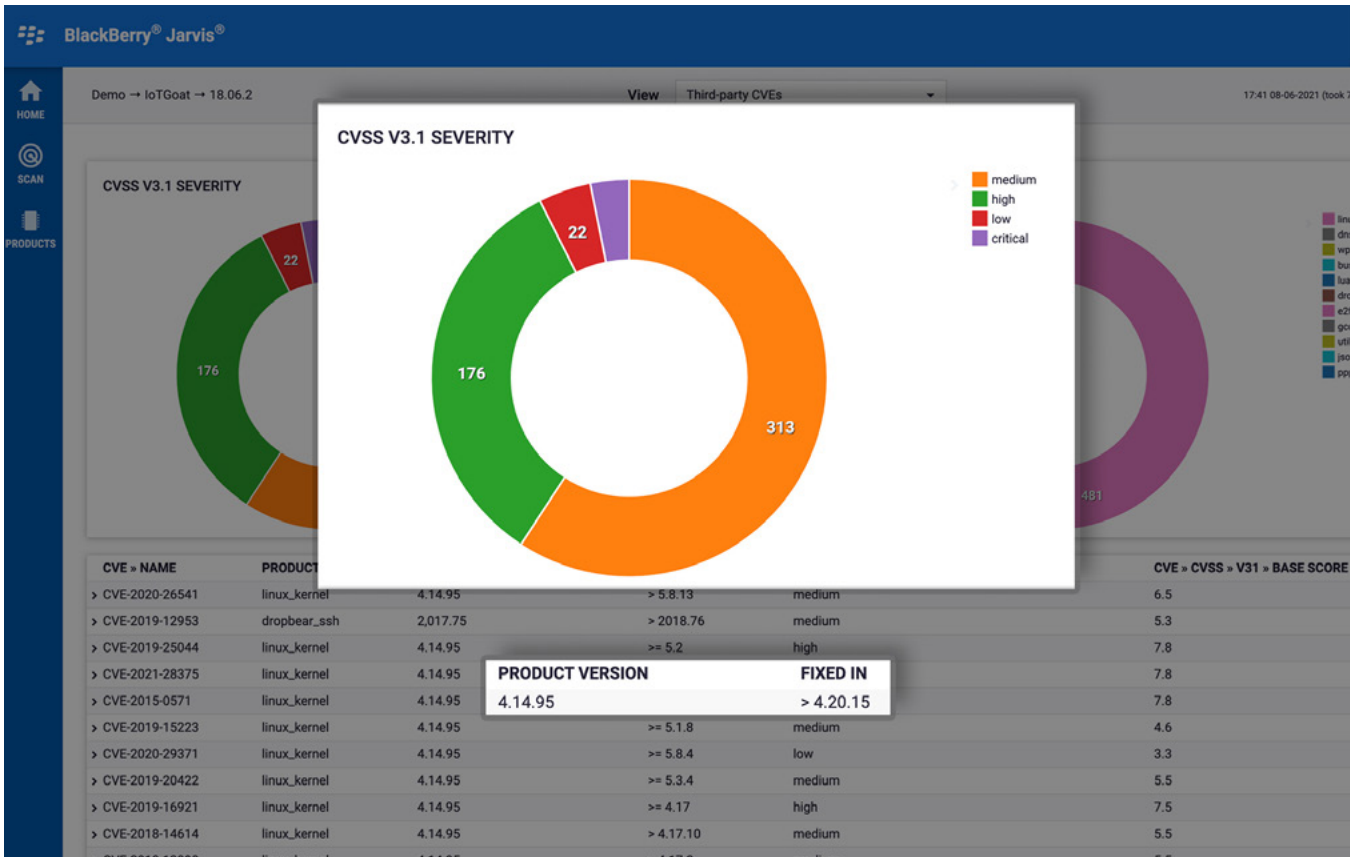

Figure 3: BlackBerry Jarvis can identify a wide variety of hardware and file types used in embedded systems. Its accurate version identification is the key to reliably uncovering vulnerabilities.

EXPERT ANALYSIS FROM BLACKBERRY QNX SECURITY SERVICES

When you have more complex needs, let BlackBerry cybersecurity experts provide further insights into your software exposure or help you improve your overall security posture. Our embedded software 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

TECHNICAL SPECIFICATIONS

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

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 our safety pre-certified product versions, is purpose built for embedded systems and scales to support everything from single-purpose devices to highly complex, mixed-criticality platforms. Because we believe we are not successful until 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 lifecycle.

PRODUCT FEATURES

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

Intuitive dashboards
Quickly identify areas of risk with CVSS scoring, allowing you to prioritize corrective actions.

Open Source Software (OSS) detection
Determine the open source software Bill of Materials (BOM) to assess associated risk and compliance.

Common Vulnerability and Exposures (CVEs)
Determine the public CVE associated with the OSSBOM using current NIST data.

Software Bill of Materials (SBOM)
Uncover potential risks hidden in the binary packages of your products. The SBOM gives you an accurate view of your products' SBOMs without reliance on information provided by suppliers.

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.