



Broadcom Strengthens Spring Security and Adds Coverage of Java, Python, and Node.js Ecosystems with TrueSource

August 31, 2026

New Offerings Expand Open Source Coverage with an Extensive Catalog of Secure, Verifiably Built, Known-good Open Source Libraries and Images

LAS VEGAS, Aug. 31, 2026 (GLOBE NEWSWIRE) -- **VMware Explore 2026** -- Broadcom Inc. (NASDAQ: AVGO), a global technology leader that designs, develops, and supplies semiconductor and infrastructure software solutions, today announced TrueSource by Broadcom, a portfolio of commercially supported, verifiably built open source software for the enterprise.

TrueSource brings together Spring Enterprise, the company's flagship offering for the Spring ecosystem; new TrueSource Trusted Artifacts, which provides secure clean-room builds of the broader Java ecosystem, Python, and Node.js and incorporates a secure catalog of hardened container images; and TrueSource Data Services, a new offering that provides trusted artifacts, support, and deployment expertise for PostgreSQL, RabbitMQ, MySQL, and Valkey data engines.

TrueSource Offerings are Built on Common Principles

- **Curated, prescriptive, enterprise-grade libraries and artifacts:** Every library and artifact is selected against a reference architecture, built, and verified by Broadcom engineers, so enterprises consume open source with confidence.
- **Remediation with maintainers, not around them:** Broadcom contributes fixes upstream and backs community maintainers across the industry with engineering time and funding.
- **Patch automation tooling and security visibility:** Automation scans customer repositories, assesses the blast radius of each release before they consume it, and opens pull requests that apply the lowest-risk remediation path, with dashboards showing their security team exactly what's fixed and what remains.
- **Early access with collaboration:** Properly licensed customers of any TrueSource offering will have the option to bring not-yet-public vulnerabilities they discover for early access to remediation. In addition, there is a special program for critical infrastructure organizations to get dedicated access to patch insights and mitigation advice.

Broadcom Sets the Enterprise Standard with Spring Enterprise

Building on Broadcom's [June commitment to Spring supply chain security](#), this announcement arrives as AI accelerates exploitation, allowing attackers to weaponize vulnerabilities in hours. While this has fueled interest in fully automated, AI-generated patching, research indicates this approach carries significant operational and security risks.

In [new testing](#), 1Password's Off-by-1 Labs found that only 26 percent of 6,000 AI-generated patches fixed vulnerabilities without breaking applications. They concluded that automated patches are not yet safe enough to trust without significant human oversight.

Spring Enterprise provides secure, curated releases of Spring from the team that creates and maintains it. That stewardship comes with over 20 years of experience in making compatibility, performance, and security judgements that have allowed Spring to flourish.

Customers receive:

- **Proactive scanning with human-verified patches:** Broadcom engineers continuously scan Spring and its dependency tree with frontier model analysis, then verify every patch by hand, finding vulnerabilities before attackers do. In the past five months, engineers have already spent more than 12 billion tokens against frontier models.
- **Simultaneous patches across every release line:** Because Broadcom maintains Spring, every supported release line is patched before a CVE is ever published. Disclosure and remediation for OSS and long term support versions arrive together, so no version is left waiting for a fix.
- **The whole dependency tree, not just Spring:** Coverage extends beyond Spring itself to its managed dependencies, including Apache Tomcat, Kotlin, and across the full dependency tree: more than 5,000 verified Java libraries, built and signed at the exact versions pinned by every supported Spring Boot release line.
- **Security fixes without the upgrade:** Full point releases bundle fixes with changes that demand testing. CVE-only patches carry the remediation alone, so security teams can push them to production in hours, not weeks.

"The world's most essential businesses run on open source software, and they trust us to keep that foundation secure," said Ram Velaga, president, Infrastructure Software Group, Broadcom. "As AI accelerates both innovation and exploitation, that trust cannot rest on unverified, machine-generated patches. It has to rest on accountable engineering. With TrueSource, we are making a long-term commitment to our customers: our fixes are built and verified by our engineers, working alongside the maintainers who know the code best."

TrueSource Trusted Artifacts Extends Coverage Across Ecosystems

TrueSource Trusted Artifacts provides secure, clean room SLSA Build Level 3 builds of libraries across the Java ecosystem, Python, and Node.js. Broadcom's curation process ensures that the libraries conform to a reference architecture and are supportable by the maintainers of record. Thousands of engineers across Broadcom's software divisions scan, fix, contribute to, and consume them every day in the software that runs the world's most essential businesses. The offering also includes the Bitnami Secure Images catalog, adding hardened, verifiably built container images for hundreds of commonly used open source packages to the same commercial offering.

TrueSource Data Services brings it to the data tier

TrueSource Data Services extends the TrueSource promise to the data engines enterprise applications depend on: PostgreSQL, RabbitMQ, MySQL, and Valkey. A flawed patch can put the data itself at risk, so remediation takes operational judgment. Broadcom brings that judgment, from hardening and supporting these engines for the world's most demanding enterprises, to curate a validated distribution inclusive of these data engines and the associated critical extensions, Operators and Helm Charts. The offering includes deployment automation for these engines as well as visibility into the security and operational posture.

One Standard Across the Portfolio

The three offerings cover different ecosystems, but they share one design: software that is verifiably built, remediated by accountable engineers, and delivered in partnership with the communities that create it. "Open source security is a human discipline," said Purnima Padmanabhan, vice president and general manager, Tanzu Division, Broadcom. "AI is a phenomenal accelerant for the engineers who maintain this software, not a replacement for them. Maintainers understand the intent behind the code, and that is what separates a real fix from one that just looks like it. TrueSource puts that human expertise at the center of the open source supply chain, at commercial scale."

"AI-generated patching, when applied outside a maintained upstream project, risks producing forks that lack maintainer oversight and long-term accountability," said Katie Norton, Research Director for IDC's Cloud Security research practice. "Broadcom's approach with Spring, pairing upstream remediation with human-verified engineering, is one response to this trend, intended to support the integrity and sustainability of the open source supply chain."

Broadcom has already invested behind this position, applying AI where it is effective. As announced in June, its Spring engineering team has scaled frontier model based scanning and validation across the dependency ecosystem, with every resulting fix authored, reviewed, and verified by engineers who know the code. That work answered the more than 1,700 percent surge in monthly security advisories reported by the Spring community and delivered the largest set of security patches in Spring's 23-year history.

Availability

Spring Enterprise, TrueSource Trusted Artifacts, and TrueSource Data Services are available with simple, tiered site licensing options.

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a technology leader that designs, develops, and supplies semiconductors and infrastructure software for global organizations' complex, mission-critical needs. Broadcom combines long-term R&D investment with superb execution to deliver the best technology, at scale. Broadcom is a Delaware corporation headquartered in Palo Alto, CA. For more information, visit www.broadcom.com.

Broadcom, the pulse logo, and Bitnami are among the trademarks of Broadcom. Postgres and PostgreSQL are registered trademarks of the PostgreSQL Community Association of Canada. MySQL is a registered trademark of Oracle Corporation. Valkey is a trademark of The Linux Foundation. All other trademarks are the property of their respective owners. Broadcom is not affiliated with, endorsed by, or sponsored by any of the foregoing organizations.

Media Contact:

John D'Avolio
Tanzu Division, Broadcom
+1.503.308.3096
john.davolio@broadcom.com