ActiveState

Three Ways Healthcare Can Secure their Software Supply Chain

Security is of paramount importance in healthcare, where personally identifiable information (PII) must be managed securely. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the US, or more generally, the General Data Protection Regulation (GDPR) in the EU, both mandate that patient health information cannot be disclosed without the patient's consent or knowledge.

But as healthcare processes and information become more and more digitized, the risk of cyberattack grows. In particular, cyberattacks on healthcare's software supply chain have been on the rise. In many of these cases, the development environment of an upstream software vendor is compromised, resulting in customers unwittingly installing malicious software that provides cyber attackers with a point of entry into their systems. Attacks of this type are much more difficult to discover and prevent than more common exploits of known vulnerabilities.

For software vendors, the ActiveState Platform provides a turnkey, end-to-end supply chain security solution. ActiveState imports source code vetted for licensing and maintainability, and then uses it to securely build the open source language packages developers need to build applications and services for the healthcare industry. And because the ActiveState Platform fits with their existing development processes, vendors can ensure the security and integrity of the software they build without incurring change costs.

Securing Healthcare Starts with a Secure Software Supply Chain

The healthcare industry is unique in being legislated to provide secure access to Electronic Health Records (EHR). This requirement imposes the need for a layer of oversight whereby healthcare institutions must closely monitor their software vendor's security posture.

But the software supply chain can be extremely complex, with hospitals (for example) requiring hundreds of software solutions and services just to maintain daily operations. When these systems are interconnected, they offer unprecedented opportunities for hackers to move laterally across critical systems.

To better protect their software supply chain, healthcare leaders and their solution vendors must work together. Some key steps healthcare should take the lead on include:

Inventory
create an inventory of all software solution vendors, from online platforms to service providers to desktop software programs.

Best Practices
have vendors fill out a questionnaire on how closely their software development processes adhere to a checklist of secure supply chain best practices.

Risk Assessment
create a risk profile for each vendor based on past performance, as well as the extent to which they have implemented secure supply chain best practices.

Software Supply Chain Security & Integrity

Securing the software supply chain starts with identifying and remediating software vulnerabilities. But for many software vendors, that's also where it ends. Vendors must identify and remediate the security and integrity flaws within the software development processes they use when importing code (such as third party software or open source components), building code (through their dedicated build and/or CI/CD systems), as well as when using/running the built artifacts.

The ActiveState Platform provides healthcare industry vendors with an out-of-the-box solution that dramatically decreases the software security and integrity threats posed by an insecure open source supply chain. The ActiveState Platform offers controls at each step along the chain, including:

Import
our open source catalog contains Indemnified Python, Perl, Ruby and Tcl packages, which have been checked to ensure they are well maintained and suitably licensed for commercial use.

Build
our secure build service features isolated, ephemeral and hermetically sealed (ie., no internet access) build steps. By taking advantage of our universal, automated build tool for Windows, Linux and macOS, developers no longer need to install potentially compromised binaries from public repositories.

Run
checksum verification of all build artifacts throughout each build step ensures that the final built package hasn't been compromised.

In this way, the ActiveState Platform delivers verifiably reproducible builds, where not only do the same inputs produce the same outputs every time, but whose provenance can also be verified by tracing each component back to its original source.

ActiveState Platform: Turnkey Supply Chain Security

The ActiveState Platform provides software vendors with a turnkey, supply chain security solution that's quick to implement, easy to use and highly automated. Rather than cobbling together custom code and a number of point solutions from multiple vendors, the ActiveState Platform can provide an out-of-the-box, end-to-end solution saving organizations considerable time, resources and money.

You can try the ActiveState Platform by signing up for a free account at
platform.activestate.com

TOYOTA NASA Honeywell CISCO NORTHROP GRUMMAN

ActiveState

www.activestate.com
Toll-free in NA: 1-866.631.4581
solutions@activestate.com

Get a Demo Contact Sales