activestate

SBOMs for Medical Device Manufacturers

Software Bill of Materials (SBOMs) provide Medical Device Manufacturer (MDMs) and their customers with a transparency mechanism that allows them to more easily track software component usage across multiple medical devices, which often contain common components.

Theoretically, this makes it easier and quicker to identify software vulnerabilities across all devices, speeding vulnerability remediation and improving device cybersecurity. Unfortunately, a lack of SBOM best practices hinder not only adoption, but Mean Time To Remediation (MTTR) of vulnerabilities, as well.

ActiveState provides a simple, standard way for any MDM to create and track SBOMs over time, as well as identify and remediate vulnerabilities quicker.

HEALTHCARE SBOM BENEFITS

The US Food and Drug Administration (FDA) has mandated that MDMs must create and maintain an SBOM for each of their devices starting October 1, 2023 due to growing security concerns associated with critical healthcare infrastructure.

Healthcare environments are all too frequently targeted by ransomware attacks because of their use of legacy platforms, as well as increasing reliance on network-connected medical devices that can all too easily get out of date because they are rarely directly update-able by healthcare staff. After all, it's not like medical providers can just shut down life-sustaining devices if they get compromised by a cyberattack.

SBOMs can help because they:

- List all the software components that comprise the application, service, API, or runtime environment on which the software in a medical device runs.
- Contain detailed information about each software component (both proprietary and third party), as well as third-party integrations.
- Provide an official record that is machine-readable.

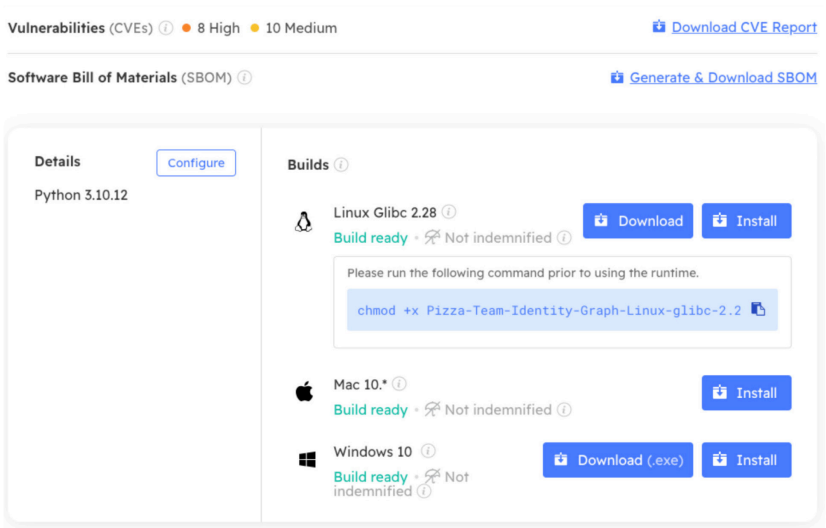
But that means healthcare providers must:

- Ensure an SBOM requirement is included in every contract for the devices they purchase.
- Employ those with the skillset to make use of SBOMs in order to be able to make informed decisions about the risks of software they deploy.
- Work with device manufacturers to expedite remediation of outdated/vulnerable components as/when identified.

At the same time, MDMs must ensure their devices are not only hardened against cyberattack, but that their firmware and software are easily updatable in the field in order to expedite vulnerability remediation.

ActiveState automatically builds Python (as well as Perl, Ruby and Tcl) runtime environments securely from

source code, and programmatically generates a JSON and SPDX SBOM for each of them. ActiveState also maintains a history of each runtime and SBOM generated, allowing MDMs to seamlessly recreate development environments (including native libraries) for devices they may have shipped years ago.



Generating SBOMs is a necessary step, but rather than just providing them to customers they can also act as a key enforcement mechanism. For example, ActiveState SBOMs can be used to:

- Verify runtime environments inside CI/CD containers to ensure the container is built with all required packages – no more, and no less.
- Verify the absence of severe or critical vulnerabilities.
- Let customers know when shipped vulnerabilities have been verified as “not exploitable” via SBOM metadata (i.e., Vulnerability Exploitability eXchange or VEX metadata).

While these capabilities can help MDMs improve the cybersecurity of the devices they ship, vulnerabilities will inevitably crop up in the field. For this reason, ActiveState also ensures that MDMs can remediate vulnerabilities quicker by:

- Flagging and notifying stakeholders when a vulnerability is detected.
- Updating an extensive catalog of open source components on a regular basis, ensuring that fixed vversions are readily available.
- Automatically rebuilding the runtime environment when a fixed version is selected, ready for testing/ deployment.

All of which can help reduce Mean Time To Remediation (MTTR) from days or weeks to a matter of hours.

ActiveState is the de-facto standard for millions of developers around the world who have been using our commercially-backed, secure open source language distributions for over 20 years. With the ActiveState Platform, developers can now automatically build their own Python, Perl or Tcl Environments for Windows, Linux or Mac—all without requiring language or operating system expertise.

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

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