CxO Trust Newsletter - July 2022

Vulnerability Management at Scale

Josh Buker, Research Analyst, CSA

Vulnerability management is a tire fire and typically a very manual process, Log4Shell being a perfect example of the problem. Every organization in the world running Java found themselves suddenly needing to track down exactly what Java applications they ship, determine if each one depended on Log4j (most did), and work overtime to ship a fix for those applications. Many teams had to burn the midnight oil over the weekend to accomplish this feat, costing significant time and money. Then, even once a vulnerability like Log4Shell is patched, there's still the problem of communicating with customers and the inevitable flood of support requests about whether you're affected or not.

Various initiatives are trying to address these issues. The need to better understand what composes the software that gets shipped has been a major component of the push for Software Bill of Materials (SBOM) and many related projects. Vulnerability-Exploitability eXchange (VEX) aims to solve the issue of communicating when and why you aren't affected by a vulnerability. Other projects have cropped up to augment initiatives like CVE, enriching it to include information like which package is affected and how bad the vulnerability is, while also making it easier to automate with tooling, saving teams time and making the process less prone to human error.

While these various initiatives are great steps forward, the data itself has become sprawled across many different sources, and discovery is a huge problem. To get the latest and greatest, the best security news feed is currently Twitter. You could also try to piece together information from dozens of different advisory databases, each with their own specific niches.

This is where the Global Security Database (GSD), an Open Source initiative from CSA, can save teams vast amounts of time and effort. By having clearly labeled machine readable data and allowing various projects to quickly and easily enrich the vulnerability data for everyone to consume, GSD allows vulnerability scanners to easily compare their known components (via SBOM) against known vulnerabilities. Rather than spending an entire weekend in a coffee-fueled craze, your teams can know in seconds if an application is affected by the most recent zero day to drop. In addition to simplifying the automation of vulnerability scanning, GSD allows security teams to have a centralized news feed to track the latest happenings in the vulnerability space.

While GSD is providing the foundation for an improved ecosystem of automated vulnerability tools, there's still much to be done. In particular, we are looking for volunteers interested in front-end development to help improve the human interface components of the project. The working group also welcomes anyone to join the discussion and help us determine the roadmap of which tools should be built out first to maximize the benefits for the industry. If you or someone on your team is interested, please sign up for the working group and join our recurring meetings every other Friday at 9:00 - 10:00 AM PDT. The next working group meeting at the time of writing will be on August 5, 2022.