VERACODE

VOLUME 12

The State of Software Security Industry Snapshot: Manufacturing

Veracode's State of Software Security (SOSS) Volume 12 examines historical trends shaping the software landscape and how security practices are evolving along with those trends. The data collected from 20 million scans across half a million applications suggests that we're making good progress toward the goal of producing more secure software.

This SOSS snapshot provides a view of software security in the manufacturing sector. We hope it brings the findings a little closer to home so you can better refine your application security (AppSec) program based on the most relevant data. Let's start things off with Figure 1, which provides some core comparative metrics for the state of software security among manufacturers.

Starting on the left, manufacturing boasts the lowest (best) rate among all industries for flaws, including high-severity flaws. The dominance ends there, however. The sector is tied for the lowest (worst) proportion of those flaws that are fixed, though the percentages show little variation among industries. This may be influenced by a larger number of specialized, industrial applications that have fewer – but harder to fix – flaws than in other industries. Regardless, identifying ways to close the fix time gap is a good action item from these results.

The rightmost columns rank industries according to how quickly they fix flaws once they're detected by three different types of scans. The manufacturing sector posts among the slowest timeframes for flaws discovered by dynamic (DAST), static (SAST), and software composition analysis (SCA) scans. These results coincide with the low fix rates previously discussed, and amplify the call for manufacturers to focus on addressing flaws in a timely fashion.

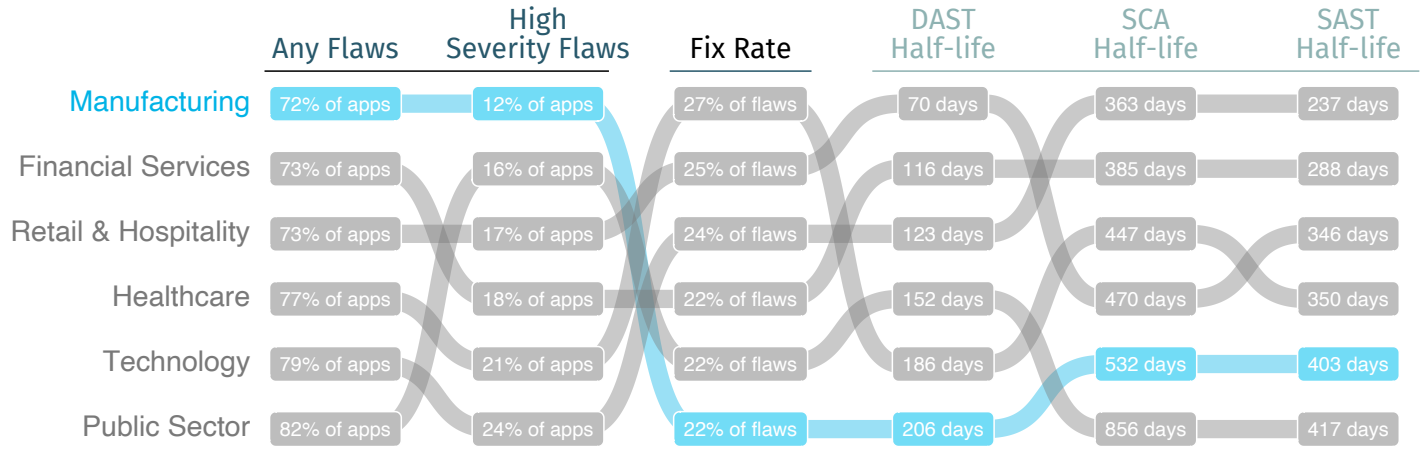

Figure 1: Values and rankings for key software security metrics by industry

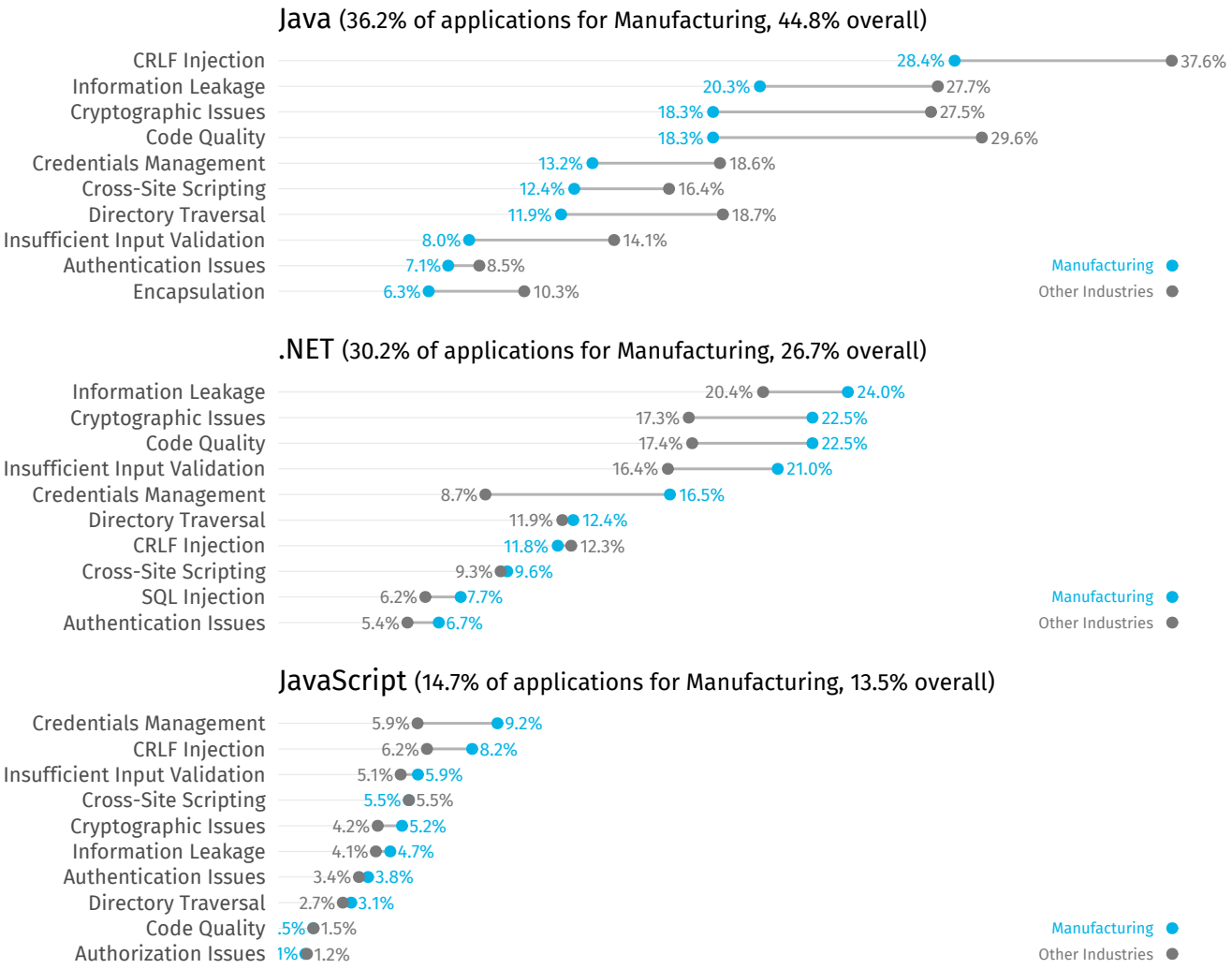

Figure 2: Most common flaws from static analysis in the manufacturing sector.

Having compared overall flaw and fix rates, let's take a look at the most common types of flaws affecting applications. Because flaws found by SAST are very language-dependent, Figure 2 separates results by the top three programming languages used among applications in the manufacturing sector. The chart makes it easy to determine whether manufacturers (in blue) have higher or lower rates than the overall average (in gray) for each type of flaw. Results are mixed here, with manufacturing beating par for Java apps and falling subpar for .NET and JavaScript. There's a lot to digest here, so we'll leave you to develop your own takeaways.

Unlike SAST, DAST findings are largely consistent across languages, leading us to combine the findings into one chart. Manufacturing follows a similar pattern to that of other industries in terms of which flaws are commonly vs. rarely identified by dynamic analysis. The percentages among manufacturers tend to be equal to or a bit higher than the average, though there are some flaw types where they're faring better (e.g., insecure dependencies and deployment configuration).

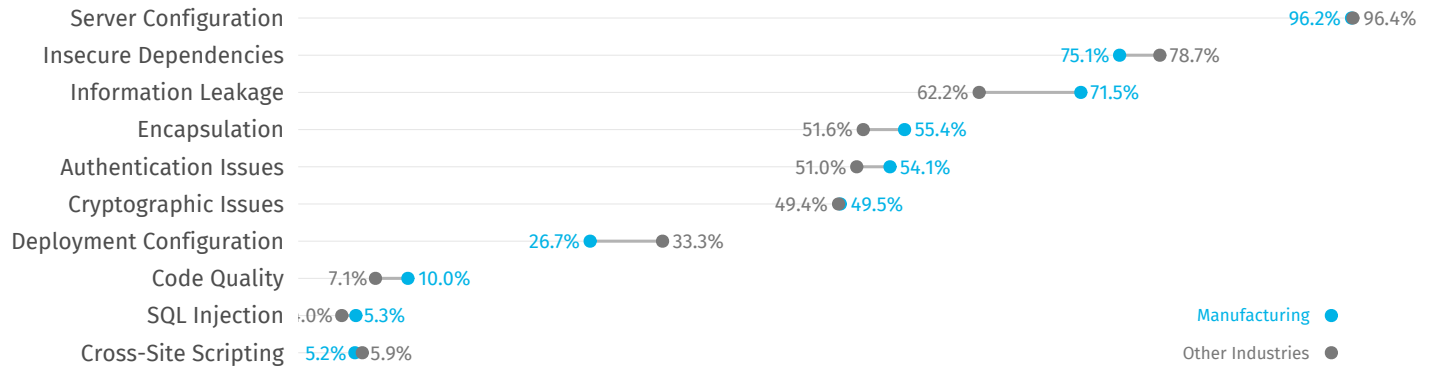

Figure 3: Most common flaws from dynamic analysis in the manufacturing sector.

Next, we'll offer a few charts that expand on the half-life stats presented back in Figure 1. The number of days required to fix half the flaws in an application is a simple, benchmark-worthy stat, but what if you're curious about the comprehensive lifecycle of software security issues? Good news – Figure 4 enables exactly that using a method known as survival analysis!

Triangulating any point along the survival curve gives the percentage of flaws still "alive" after a period of time following discovery (e.g., ~55 percent still unresolved after one year). The manufacturing sector is experiencing some challenges here, consistently lagging four months behind the overall average across the entire lifecycle of software flaws according to SAST. For DAST, manufacturers lag early on but manage to catch up and outpace others in the long run.

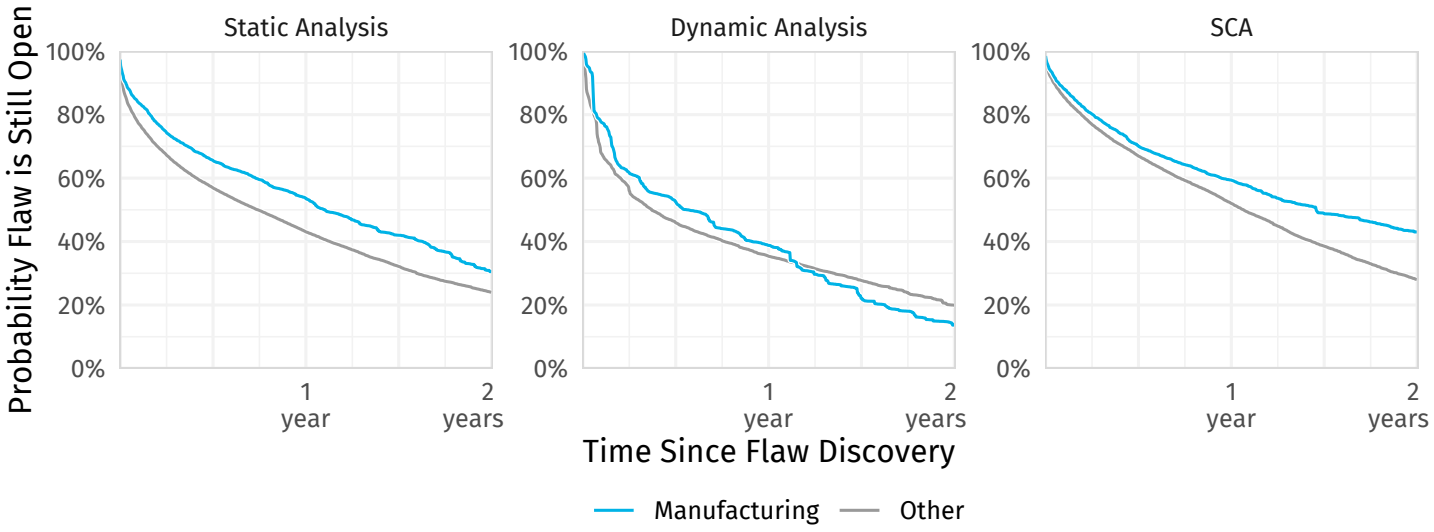

Figure 4: Two-year flaw survival rates for applications in the manufacturing sector.

Flaws in third-party libraries found through SCA stick around longer for all industries, and even longer among manufacturers. Overall, about 30 percent of vulnerable libraries remain unresolved after two years. For the manufacturing sector, that statistic rises to over 40 percent and lags the cross-industry average by over six months.

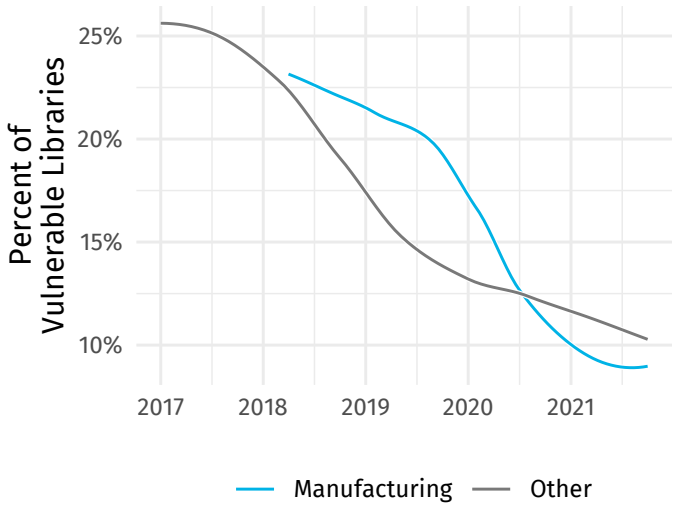

Figure 5: Proportion of vulnerable libraries used by applications in the manufacturing sector.

Speaking of vulnerable libraries, you're probably aware that the software supply chain is kind of a big deal these days. This last chart shows the extent of flaws in third-party code discovered via SCA. The ratio trends down over time, with manufacturers initially higher than the overall average and dipping below over the last year or so. It's nice to end on a good note, and we hope retailers see this as a welcome ray of sunshine amidst the all-too-often gloomy realm of software security. Here's to more clear skies in the years to come!

VERACODE

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at **www.veracode.com**, on the **Veracode blog**, on **LinkedIn**, and on **Twitter**.

Read the Full Report