VOLUME 12

The State of Software Security Industry Snapshot: Public Sector

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 public 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 in the public sector.

Starting on the left, the public sector owns the highest proportion of applications exhibiting any flaws but rank much better for the most severe flaws. If you can't fix them all (and nobody can), then those are definitely the subset to prioritize. The sector falls back down the rankings when it comes to the proportion of security flaws that are fixed, though there's little variation here. It appears that all organizations, the public sector included, would benefit from efforts to address software flaws in a more comprehensive manner.

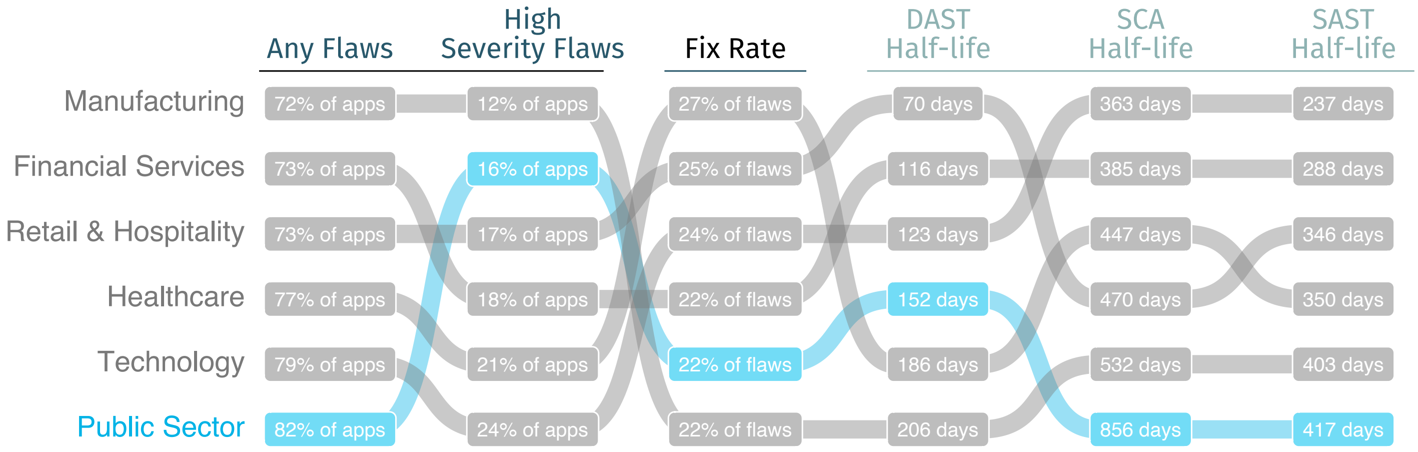

Figure 1: Values and rankings for key software security metrics by industry.

The rightmost columns rank industries according to how quickly they fix flaws once they're detected by three different types of scans. The public sector posts on the slower end of timeframes for flaws discovered by dynamic analysis (DAST) and dead last for static analysis (SAST) and software composition analysis (SCA) scans. These results coincide with the low fix rates previously discussed and amplify the call for agencies to address flaws in a timely fashion.

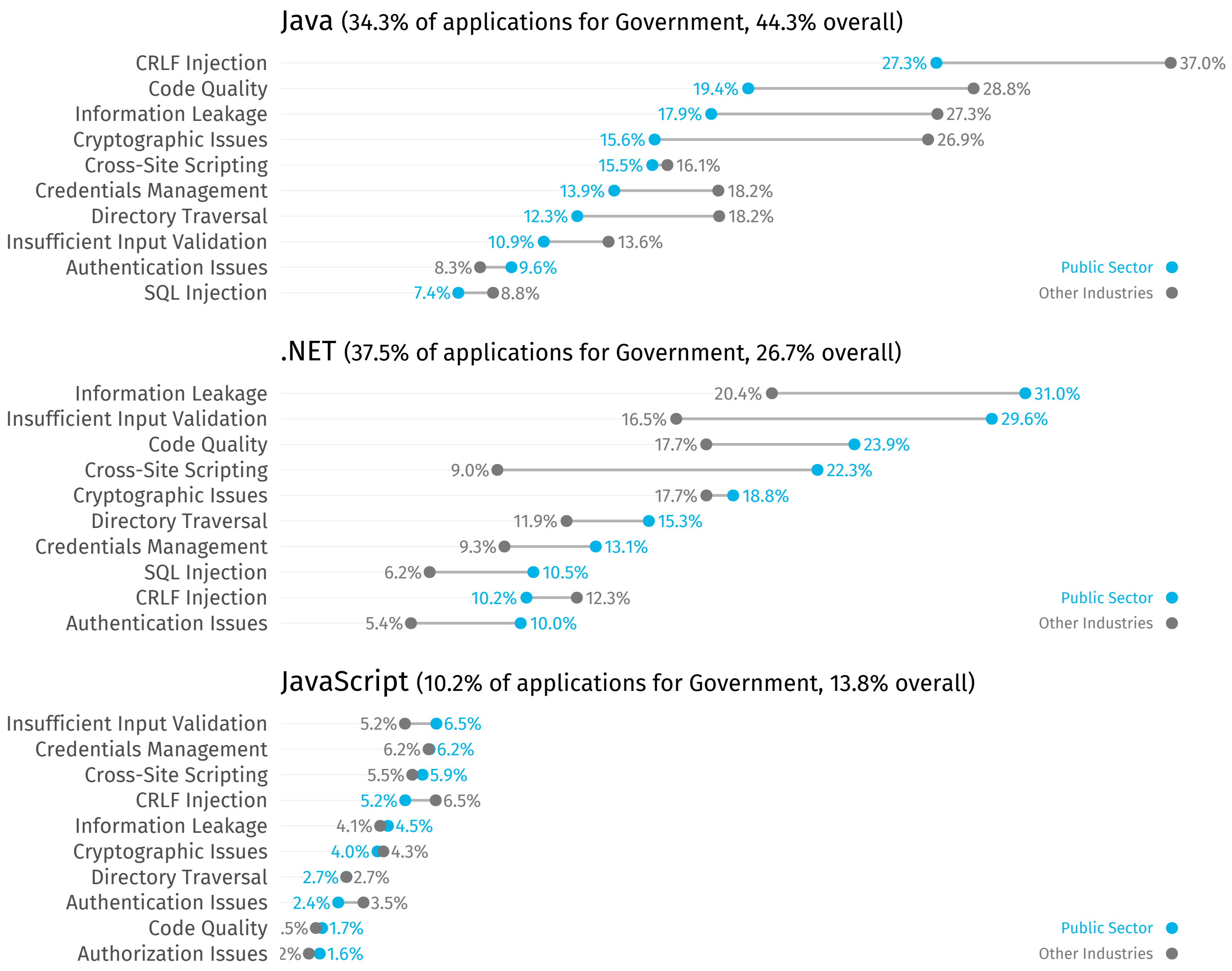

Figure 2: Most common flaws from static analysis in the public sector.

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 public sector. The chart makes it easy to determine whether the public sector (in blue) has higher or lower rates than the overall average (in gray) for each type of flaw. Results are mixed here, with the public sector beating par for Java apps, subpar for .NET, and about par for 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. The public sector follows a similar pattern to that of other sectors in terms of which flaws are commonly vs. rarely identified by dynamic analysis. The percentages for the public sector are higher for all categories, however, it could be due to historically larger applications with greater functional complexity.

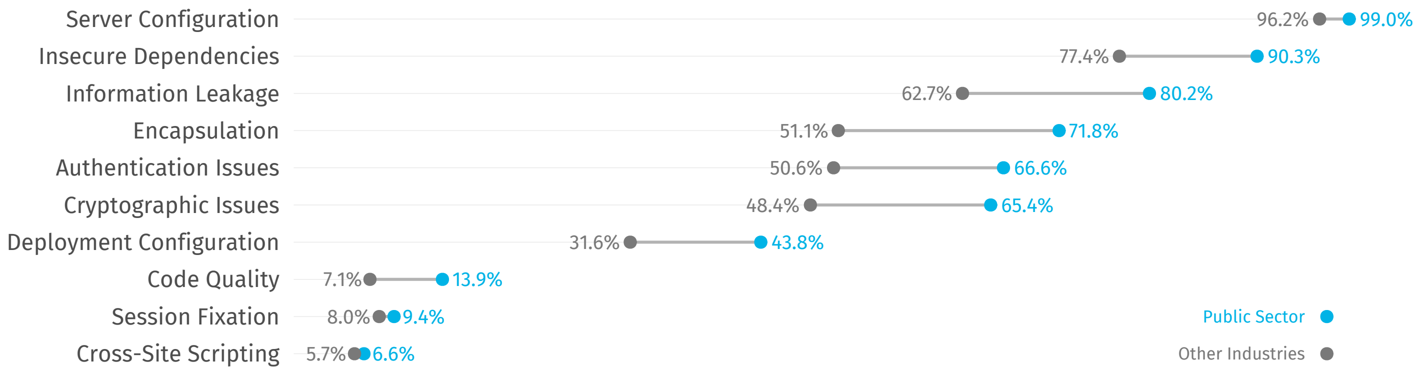

Figure 3: Most common flaws from dynamic analysis in the public sector.

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 public sector is experiencing some challenges here. The public sector is consistently four months behind the overall average across the entire lifecycle of software flaws according to SAST. For DAST, agencies lag early on but manage to catch up and outpace others in the long run.

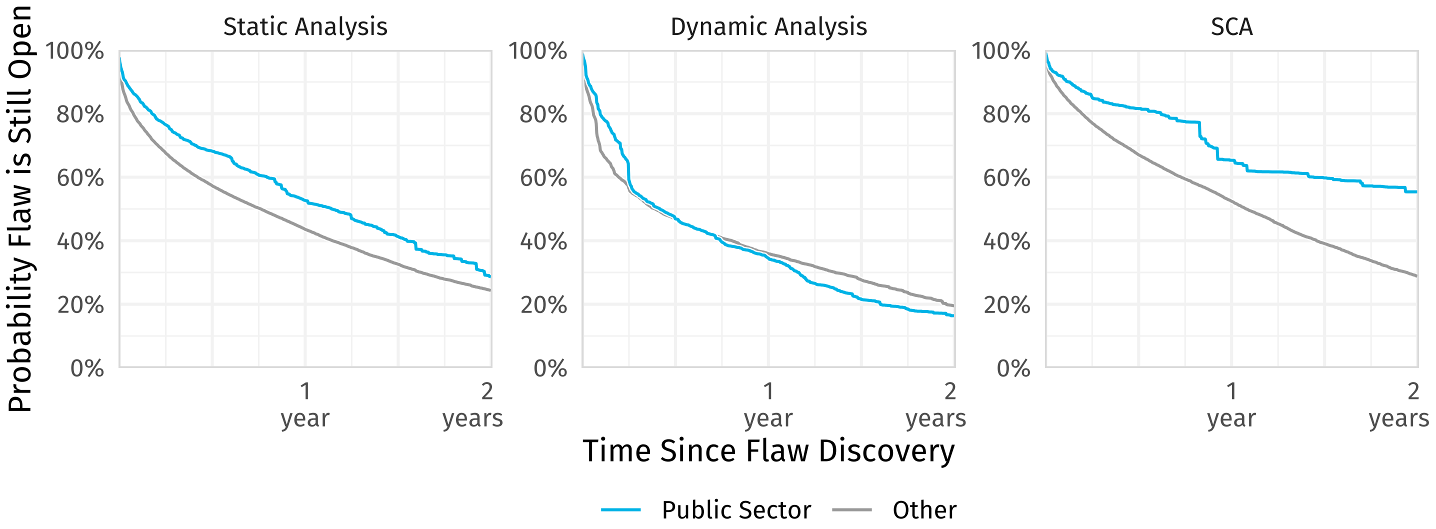

Figure 4: Two-year flaw survival rates for applications in the public sector.

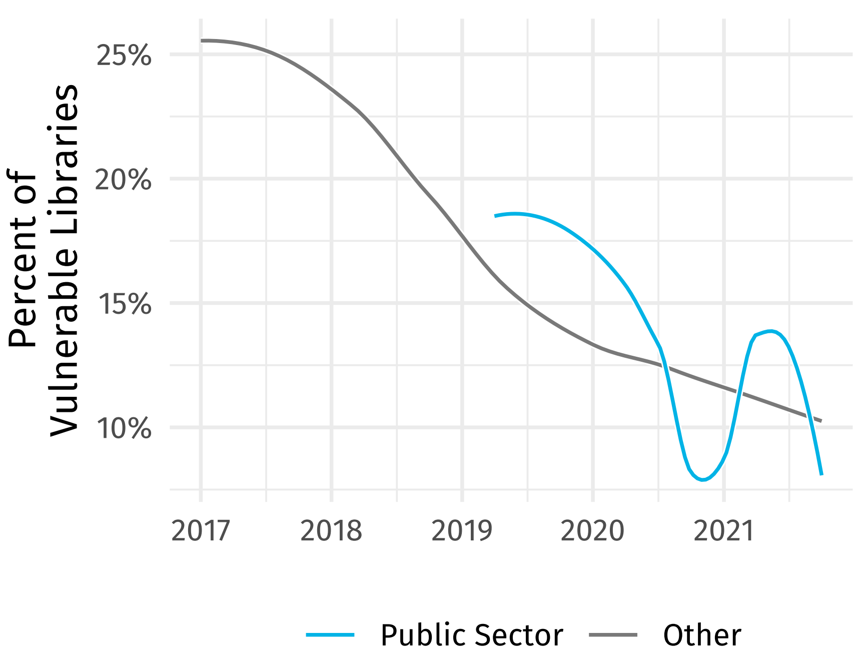

Figure 5: Proportion of vulnerable libraries used by applications in the public sector.

Flaws in third-party libraries found through SCA stick around longer for all industries, and even longer in the public sector. Overall, about 30 percent of vulnerable libraries remain unresolved after two years. For the public sector, that statistic doubles to almost 60 percent and lags the cross-industry average by over 15 months.

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 overall ratio trends down over time. Rates for the public sector show some ups and downs but are at least trending in the right direction. We hope public sector developers and IT staff 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