VERACODE

VOLUME 12

The State of Software Security Industry Snapshot: Healthcare

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 healthcare 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 healthcare.

Starting on the left, healthcare providers rank toward the bottom in terms of proportion of applications with any security issues as well as with high-severity flaws. The industry takes first place for the highest proportion of those flaws that are fixed, though the percentages are quite low across the board and show little variation. It appears that all organizations, healthcare included, would benefit from efforts to address software flaws in a more comprehensive manner.

The rightmost columns rank industries according to how quickly they fix flaws once they're detected by three different types of scans. The healthcare sector posts middle-of-the-road fix times for flaws discovered by static (SAST), dynamic (DAST), and software composition analysis (SCA) scans. Certainly not the worst among industries, but the number of days required to get to the halfway point shows there's ample room for continued improvement by healthcare providers.

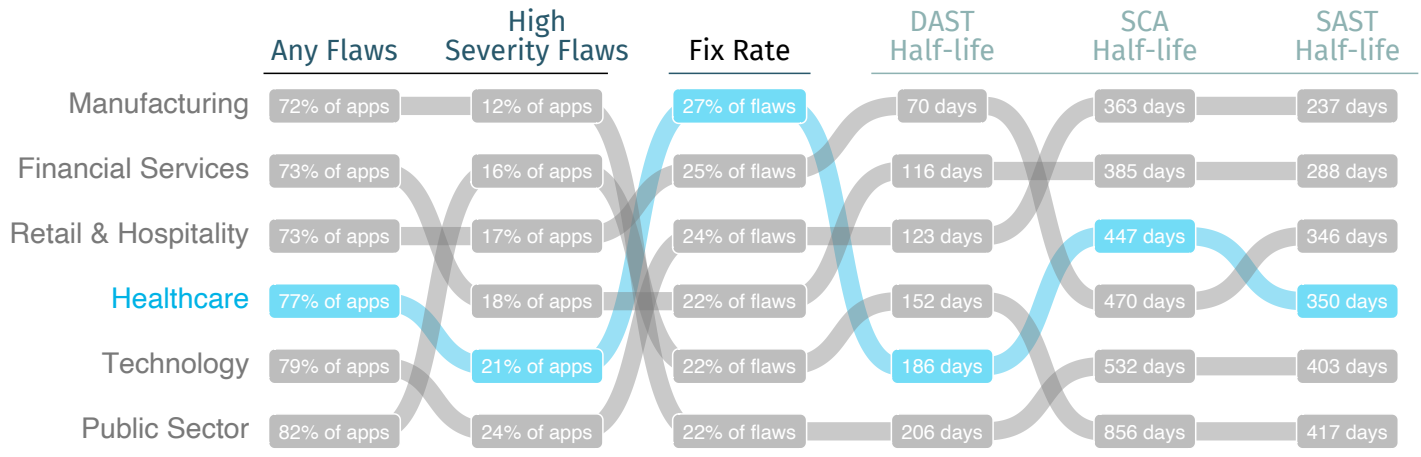

Figure 1: Values and rankings for key software security metrics by industry

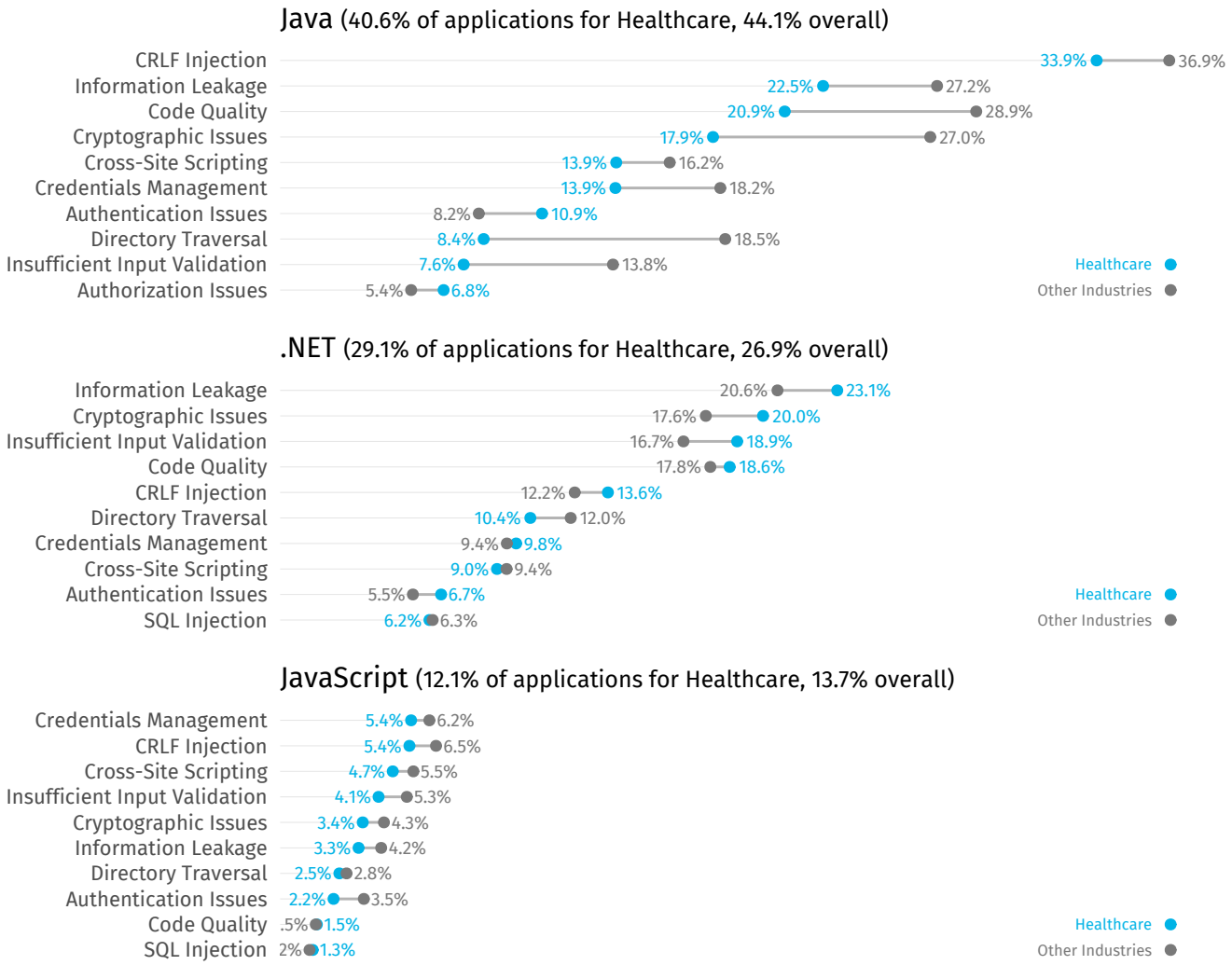

Figure 2: Most common flaws from static analysis in the healthcare sector.

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 healthcare sector. The chart makes it easy to determine whether healthcare providers (in blue) have higher or lower rates than the overall average (in gray) for each type of flaw. Results are mixed here, with healthcare typically scoring better than par for Java and JavaScript apps and subpar for .NET. 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 healthcare industry follows a similar pattern to that of others in terms of which flaws are commonly vs. rarely identified by dynamic analysis. Healthcare providers are doing comparatively well with authentication issues and insecure dependencies, while posting higher rates for cryptographic and deployment configuration issues.

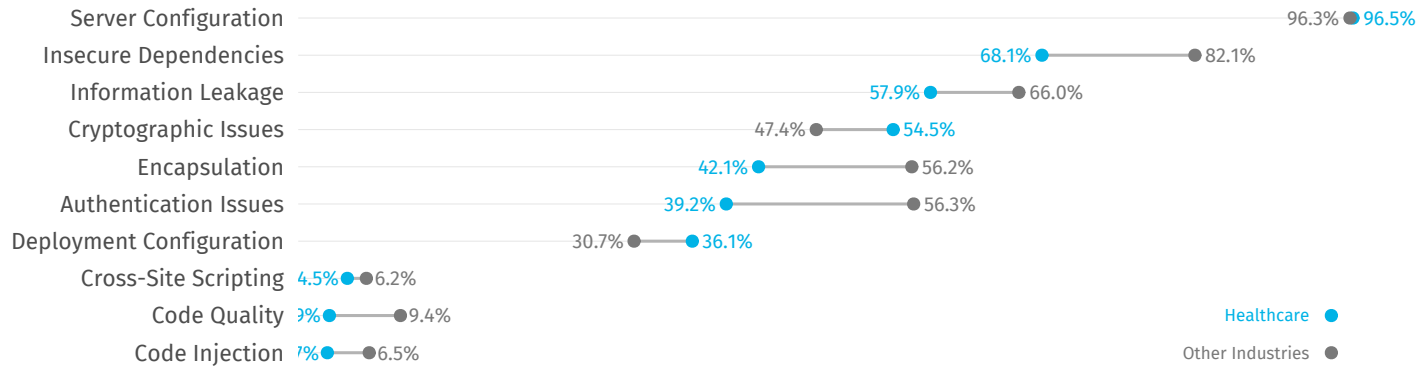

Figure 3: Most common flaws from dynamic analysis in the healthcare sector.

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., ~60 percent unresolved after six months). The healthcare sector is experiencing some challenges here, lagging about three months behind the overall average across much of the lifecycle of software flaws according to SAST. For DAST, healthcare lags early on but manages to catch up and slightly outpace others in the long run.

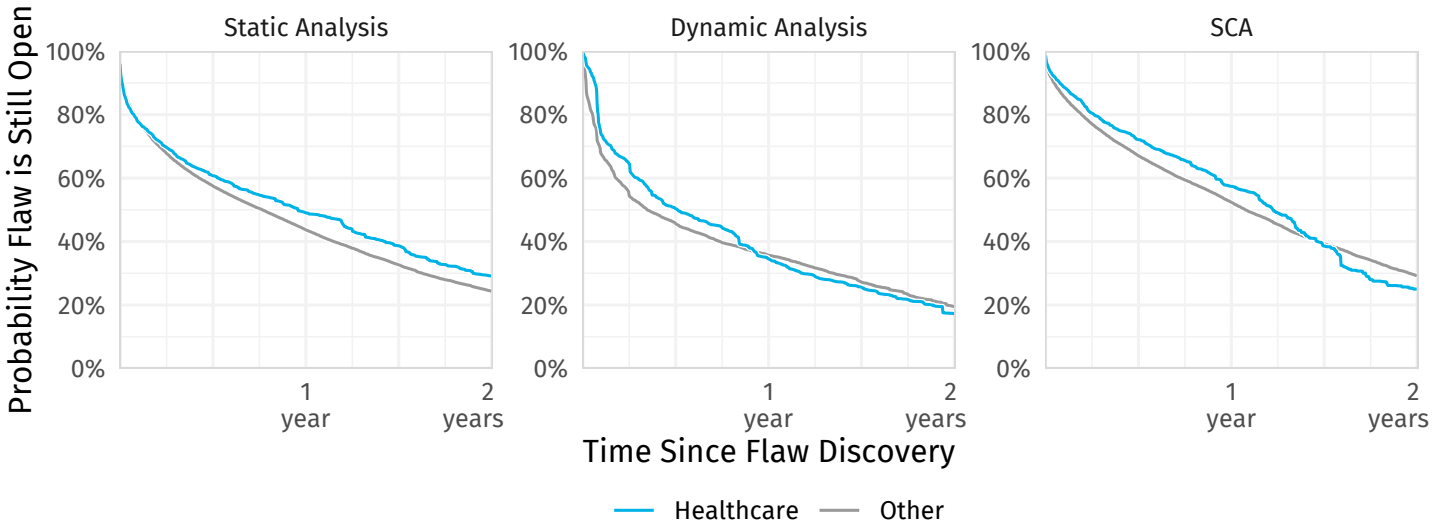

Figure 4: Two-year flaw survival rates for applications in the healthcare sector.

Flaws in third-party libraries found through SCA stick around longer for all industries, and even longer (at least initially) among healthcare providers. Overall, about 30 percent of vulnerable libraries remain unresolved after two years. That statistic edges down to 25 percent for the healthcare sector, thanks to a relatively quicker pace down the backstretch in year two.

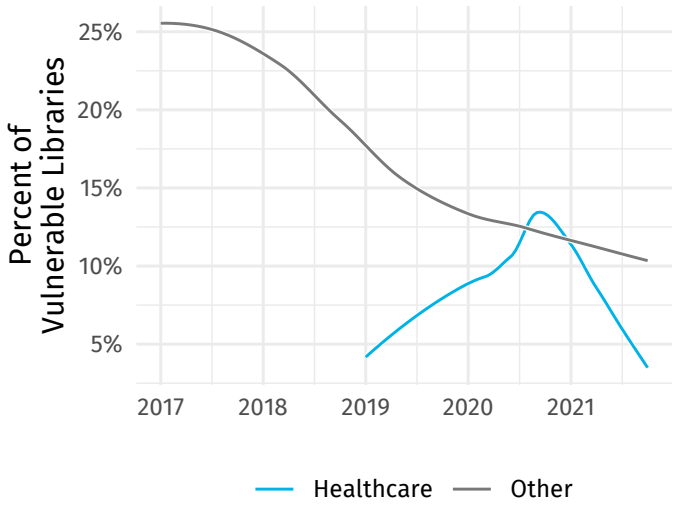

Figure 5: Proportion of vulnerable libraries used by applications in the healthcare sector.

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 overall ratio trends down over time, with healthcare experiencing a bit of a bump before driving rates down over the last year or so. We hope healthcare 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!

Read the Full Report