VERACODE

VOLUME 12

The State of Software Security Regional Snapshot: Europe

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. This infosheet provides a summary of the factors that shape software security for European firms compared to their global brethren.

Figure 1 provides some core comparative metrics for the state of software security across regions. Starting on the left, European organizations rank in the lower half among regions for both overall flaw percentage and high-severity flaws. The region edges into the middle of the pack for the proportion of those flaws that are fixed, though the percentages show little variation among regions (baring Asia). Overall, the first three columns suggest that many European firms would benefit from finding and fixing their most critical flaws.

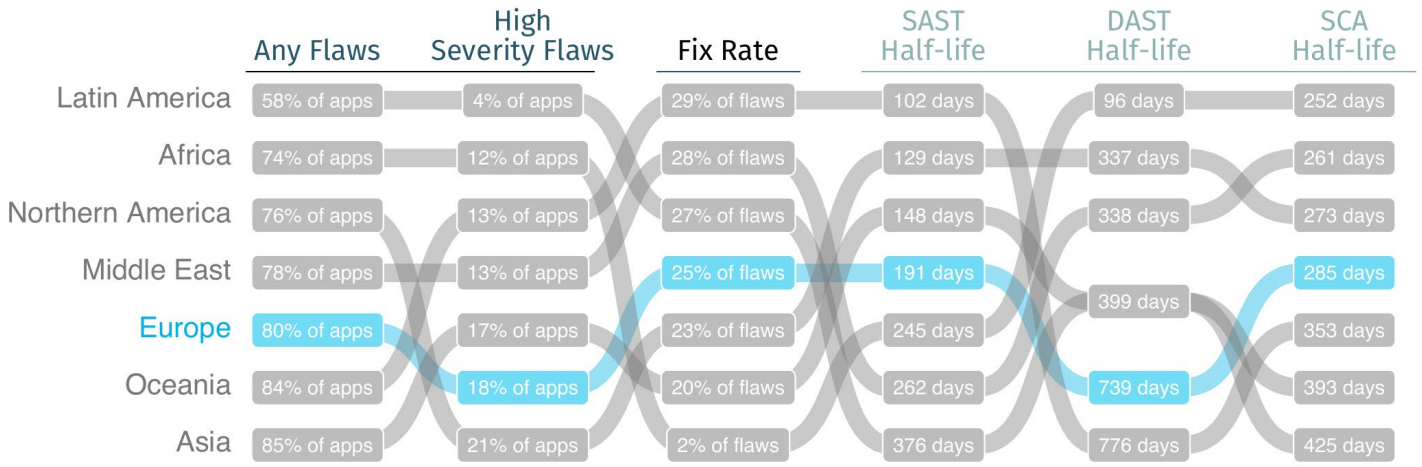

Figure 1: Values and rankings for key software security metrics by industry

The rightmost columns rank industries according to how quickly they fix flaws once they're detected by three different types of scans. Europe posts middling fix times for flaws discovered by static (SAST), dynamic (DAST), and software composition analysis (SCA) scans. Certainly not the worst among regions, but the number of days required to remediate 50 percent of flaws shows that there's ample room for continued improvement by European organizations.

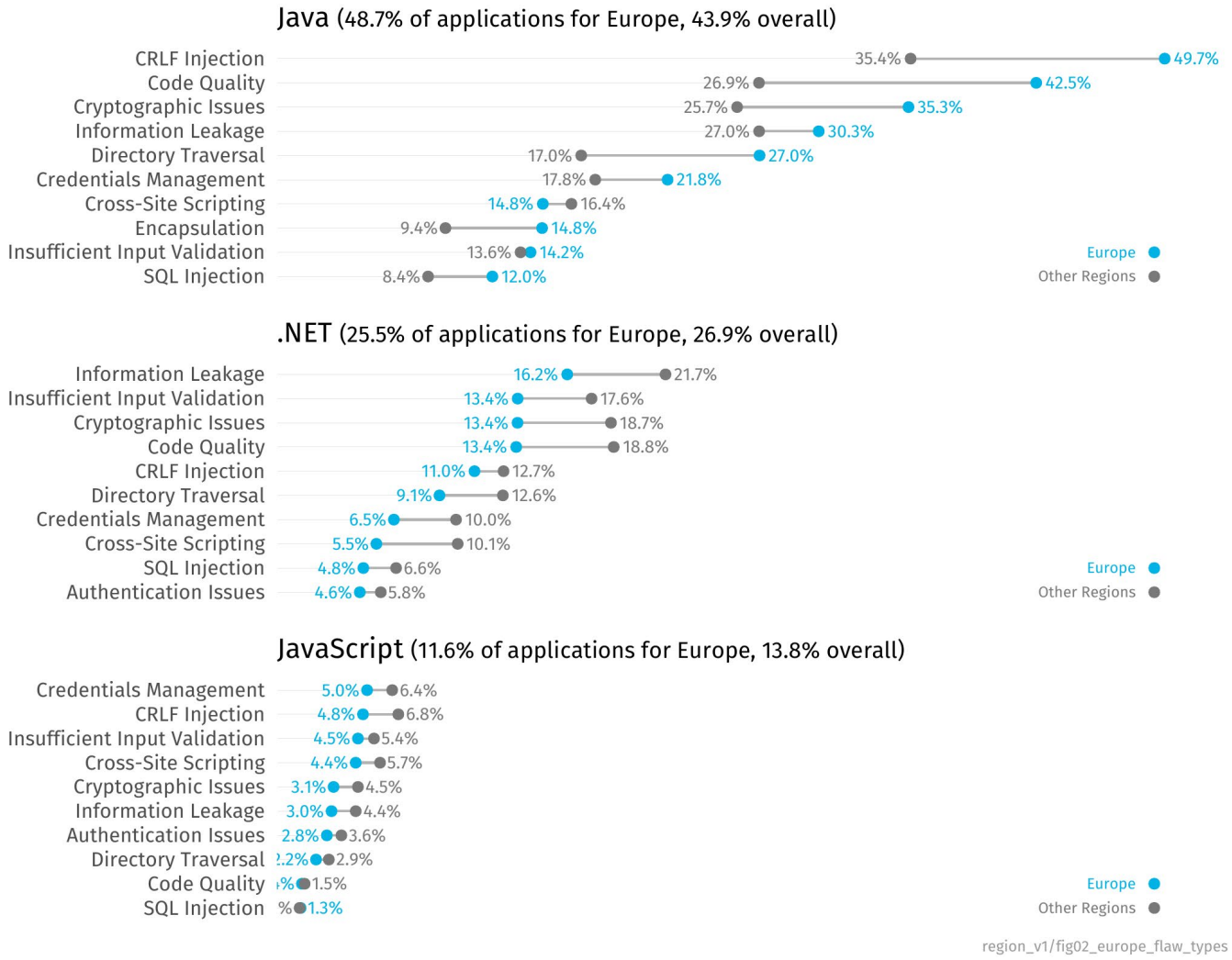

Figure 2: Most common flaws from static analysis of software in the European region

Having compared overall flaw and fix rates, let's take a look at the most common types of flaws impacting applications. Because flaws found by SAST are very language-dependent, Figure 2 separates results by the top three programming languages used in applications in Europe. The chart makes it easy to determine whether European organizations (in blue) have higher or lower rates than the overall average (in gray) for each type of flaw. Results are mixed here, with the region generally exhibiting higher flaw rates for Java and lower for .NET and JavaScript. There's a lot of information to digest, 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. Europe largely follows a similar pattern to that of others in terms of which flaws are commonly vs. rarely identified by dynamic analysis. The region is doing comparatively well for cryptographic and deployment configuration issues, while flaws associated with information leakage and encapsulation tend to be a bit higher.

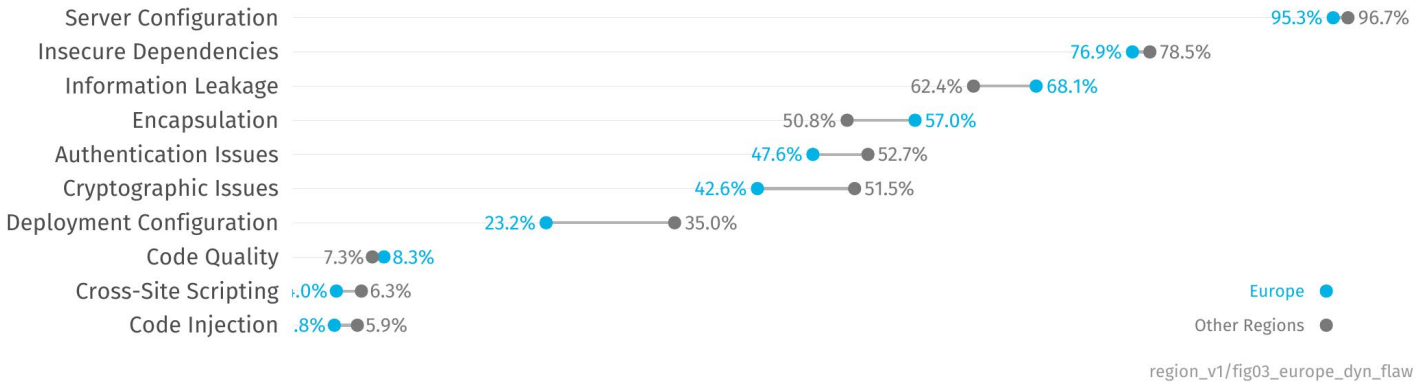

Figure 3: Most common flaws from dynamic analysis of software in the European region

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 shows 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., over 40 percent still unresolved after one year). The lifecycle of application flaws found via SAST by European firms tracks closely with the global average, though the region does pull slightly ahead down the stretch. On the other hand, Europe is a bit behind the curve when it comes to addressing DAST-sourced flaws.

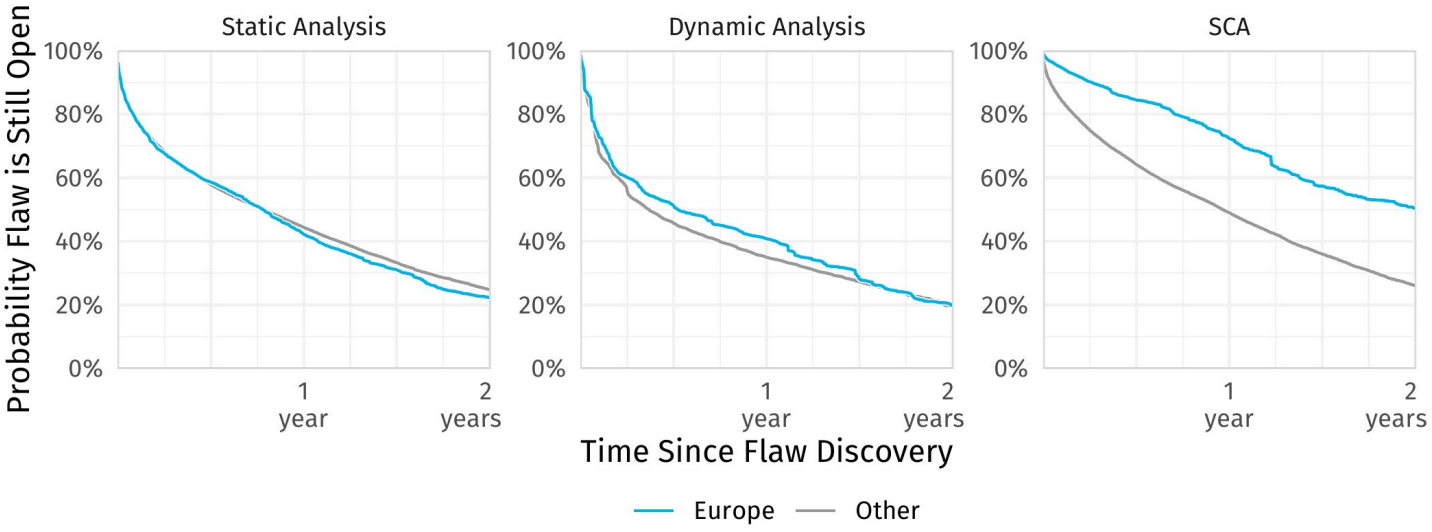

Figure 4: Two-year flaw survival rates for applications in the European region

Flaws in third-party libraries found through SCA stick around longer for all industries, and even more so for European organizations. Overall, about 30 percent of vulnerable libraries remain unresolved after two years. For the public sector, that statistic jumps to 50 percent and lags the cross-industry average by 12 months.

Speaking of vulnerable libraries, you're probably aware that the software supply chain is kind of a big deal these days among software security professionals. The last set of charts in this snapshot show the extent of flaws in third-party code discovered via SCA. Java applications exhibit the highest ratio of vulnerable libraries, but that's trending down over time. The same can be said for the other languages, which is a welcome ray of sunshine in an otherwise gloomy realm of software security. Here's to increasingly clear skies ahead in the years to come!

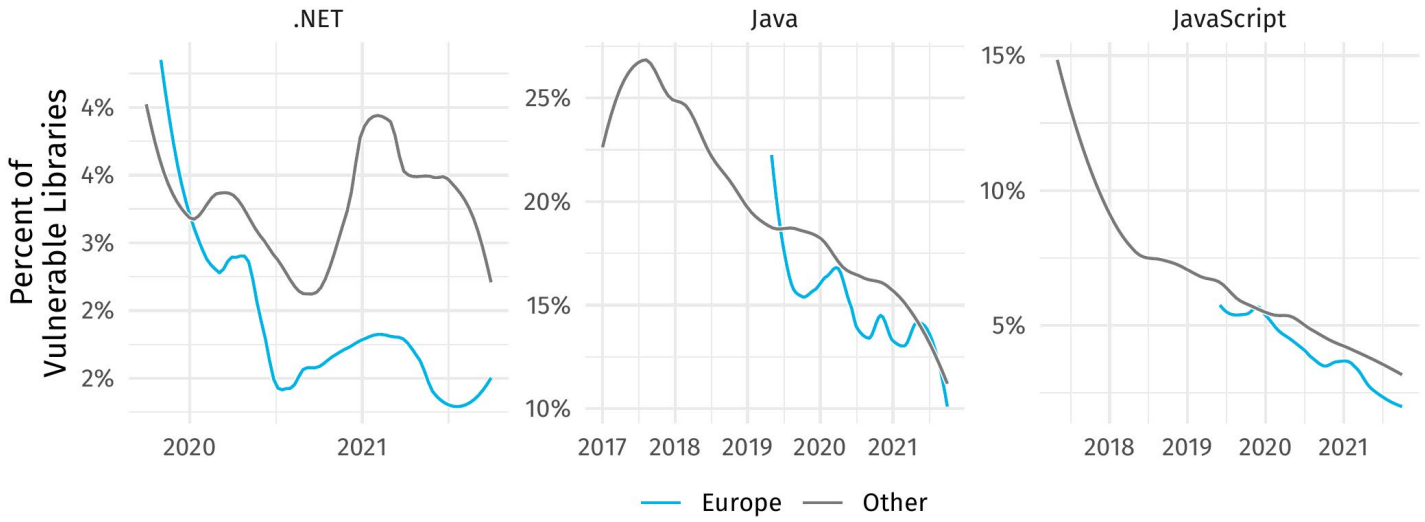

Figure 5: Proportion of vulnerable libraries used by applications in the European region

VERACODE

Veracode is the 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 automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.Veracode serves thousands of customers worldwide across a wide range of industries. The Veracode solution has assessed more than 45 trillion lines of code and helped companies fix more than 68 million security flaws.

www.veracode.com **Veracode Blog**

Read the Full Report