VERACODE

VOLUME 11

The State of Software Security
Industry Snapshot: Manufacturing

Veracode's State of Software Security (SOSS) Volume 11 focused on how developer actions can influence software security. It also looked at the impact that application attributes (their "nature") and the development environment (the "nurturing" of the app) can have on how quickly flaws are fixed. Our analysis uncovered key differences in software security between industries and found that these differences affect how quickly flaws were addressed, adding another dimension to our "nature vs. nurture" discussion. This infosheet provides a summary of factors that shape software security for the manufacturing sector.

Figure 1 describes how applications compare across industries in finding and fixing flaws. From left to right, the columns rank each industry by proportion of applications with flaws, the proportion of applications with high-severity flaws, the percentage of flaws that are fixed, and the median speed at which flaws are fixed. Manufacturing is tied for middle on the overall proportion of applications with flaws but jumps to the front of the class with the lowest proportion of applications with high-severity flaws. The remediation side of this figure shows where the industry is struggling: Manufacturing ranks last both for the overall fix rate and the median time to remediate flaws. With the slow cycles found in many industrial control and embedded systems, these results are not unexpected, though still disappointing.

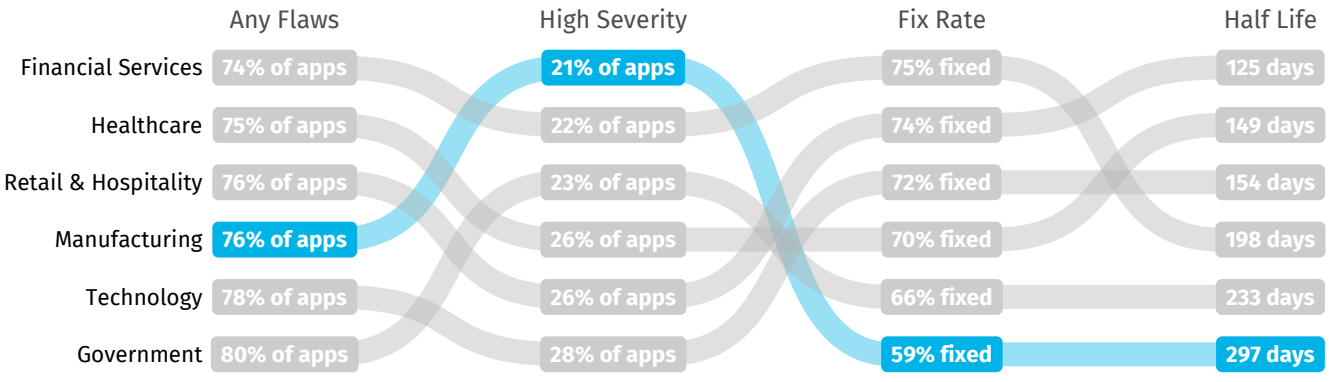
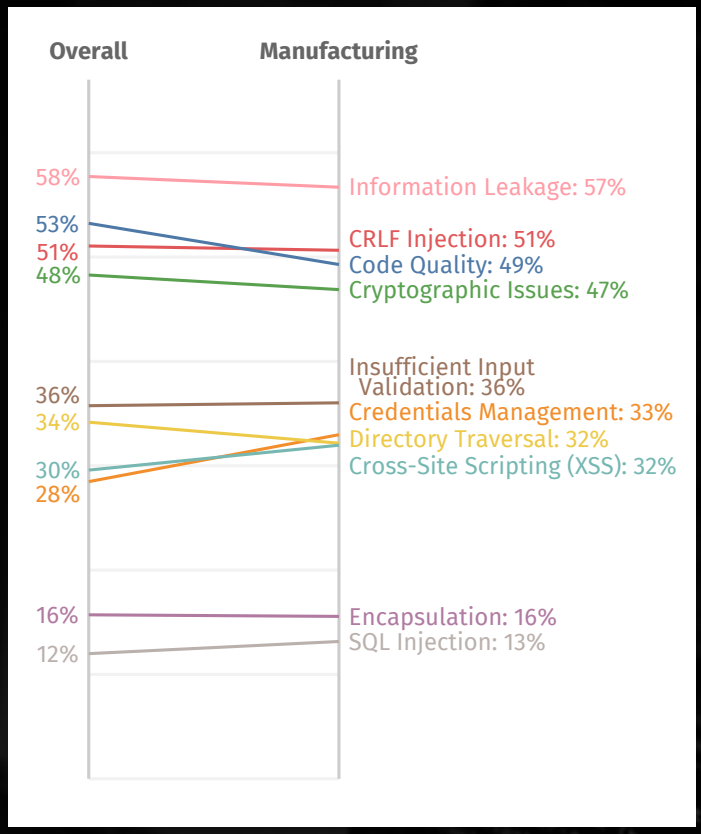


Figure 1: Values and rankings for key software security metrics by industry.

In Figure 2, we show a more detailed view of the flaw types discovered in applications. The left axis shows the overall prevalence of each flaw category across all sectors, and the right axis shows the prevalence of the category for the manufacturing industry. The figure shows that the prevalence of these common flaw types tends to be roughly in line with the overall trends. An exception is credential management, as those issues are found more often in this sector than on average. Historically, many applications in manufacturing did not require authentication, so that may explain some of the difficulties. Code quality stands out as a flaw type found less often in this sector than on average. Perhaps it is the rigor of the engineering disciplines making their presence known here?

In this year's SOSS, we see strong evidence that certain developer behaviors associated with DevSecOps yield substantial benefits to software security. In Volume 10, we discovered that teams scanning applications most frequently carry five times less security debt than infrequent scanners. In this volume, we see other developer actions also make a difference in fixing flaws in software.

For example, we looked at the impact that application attributes and the development environment can have on how quickly flaws are fixed in software. There are some attributes that developers have no control over and others, such as best practices, that developers can influence.



Prevalence of flaw categories in the manufacturing sector

In Figure 3, we look at how manufacturing companies compare with companies in other industries in their development attributes (nature) and utilizing helpful developer behaviors (nurture). The data shows that manufacturing firms have a mix of middle- and bottom-of-the-pack behaviors and attributes. The development environment is challenging for manufacturing firms, as their applications tend to be slightly older than those in other industry sectors and the organizations on the larger end.

Their applications are often larger than those found in any other sector with one of the highest density of flaws in our sample. Behaviors are similarly mixed, with manufacturing firms reaching overall middle-of-the-pack performance on their use of DAST and scanning cadence, but at or near the bottom for scanning frequency, API usage, and software composition analysis (SCA) compared to other industry sectors. This suggests that for many manufacturing firms, developers face a challenging environment, with the adoption of additional DevSecOps practices showing the most opportunity for improvement.

In the most recent SOSS, we see that certain factors are likely to lead to flaws getting fixed faster, and others lead to slower fixes. Industry is something developers don't have control over, so how does being part of the manufacturing industry affect time to remediate flaws?

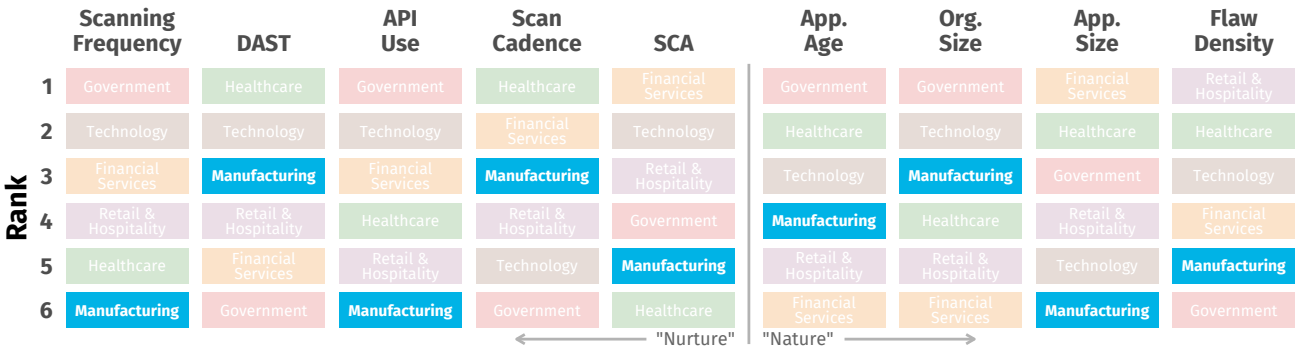


Figure 3: Relative ranking of the manufacturing sector for attributes and actions associated with application security performance

It's slower. Figure 4 shows us that being in the manufacturing industry means the firm is more likely to be slow in remediating flaws. We saw in Figure 3 that developers in manufacturing are dealing with a challenging environment and are not consistently following DevSecOps practices compared to other industries. The combined effects of nature and nurture indicate remediation efforts among manufacturing firms tend to be less effective, and that flaws are fixed slowly. This may partially explain why the median time to remediation back in Figure 1 was so long. It goes to show that when developers can't control their environment and don't adopt best practices for secure coding, there is a negative impact on software security.

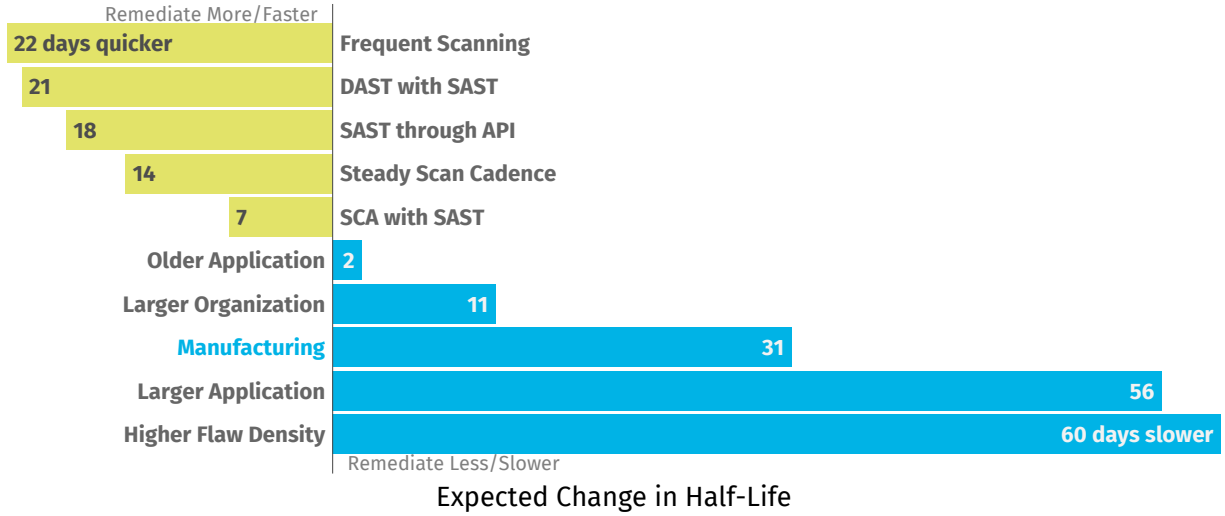


Figure 4: Remediation factors...

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 more than 2,500 customers worldwide across a wide range of industries. The Veracode cloud platform has assessed more than 14 trillion lines of code and helped companies fix more than 46 million security flaws.

www.veracode.com Veracode Blog Twitter

Read the Full Report

TO LEARN MORE ABOUT SOFTWARE SECURITY, CONTACT US.