

EXECUTIVE SUMMARY

2021 Application
Security
Observability
Report

Data from the Entire SDLC

Contrast Labs' second annual Application Security Observability Report takes a broad look at the state of application security at a critical moment in the economy—as businesses reopen their office locations and discern the next phase of how work is structured. The data comes from aggregate telemetry from applications and application programming interfaces (APIs) protected by the Contrast Application Security Platform. It includes data on vulnerabilities, attacks, and open-source libraries between June 2020 and May 2021. New data introduced this year includes calculations of the vulnerability escape rate (VER) and the number of routes exercised by applications. Such comprehensive reporting from across the software development life cycle (SDLC) is only available from Contrast Security.

Application Makeup is Surprising

The fact that 70% or more of the code in the typical application comes from open-source libraries and frameworks has been widely noted in recent years. What is not usually revealed in these reports is that the vast majority of this code is not used by the application. Our data shows that 80% of code is open source, but 74% of that code is inactive—belonging either to an inactive library or an inactive class within an active library.

As a result, just 6% of the total code in the typical application is open-source code that is invoked by the application. When this is taken into account, it becomes clear that 77% of active code in the typical application is custom code and that only 23% comes from open sources. Looking at it from that perspective, custom code becomes much more important to the application security mix.

This data on application makeup dramatically impacts an organization's strategy for dealing with Common Vulnerabilities and Exposures (CVEs) in their open-source code. The fact is that CVEs in inactive code pose no risk to an organization. Traditional software composition analysis (SCA) tools do not differentiate between active and inactive code. As a result, every CVE they identify that occurs in inactive code is actually a false positive. In our dataset, a majority of vulnerabilities—including 54% of CVEs rated as Critical and 49% rated as Major—would be false positives with traditional tools.

APPLICATION MAKEUP

20%

Custom Code

6%

Active Library Classes

74%

Inactive Libraries and
Inactive Classes Within
Active Libraries

FALSE POSITIVE RATE

54%

for Critical CVEs

49%

for Major CVEs

More Custom Code Vulnerabilities are Serious

Given this importance, it is concerning that more custom code vulnerabilities are serious than last year. Most concerning is an increase in the percentage of applications with at least one serious vulnerability, defined as High or Critical—34% this year compared with 26% last year. This means that serious vulnerabilities increased by 19% as a share of all vulnerabilities. And while 13% of applications have just one or two serious vulnerabilities, 3% have more than 100. Overall, 39% of all vulnerabilities identified are serious compared with 28% last year—a 39% increase.

The top two vulnerability types in terms of percentage of applications affected are broken access control and cross-site scripting (XSS). Unfortunately, both of these vulnerability types were found in a larger share of applications this year than last year. As in the past, more Java applications have serious vulnerabilities than .NET ones—44% versus 23%.

34%

of Applications Have a Serious Vulnerability (19% increase from 2020)

39%

of Vulnerabilities Are High or Critical (39% increase over 2020)

17%

of Applications Are Impacted by Broken Access Control and XSS Vulnerabilities

13%

of Applications Have at Least 1 Serious Vulnerability; 3% have 100+

Vulnerability Escape Rate Decreases Over Time

The good news is that Contrast enables developers to improve the security of their coding over time. With its immediate feedback when a vulnerability is created, the platform provides actionable instructions on how to fix the problem—and avoid making the same mistake again in the future. The result is akin to “just-in-time” security training—something that learning managers have struggled to provide for developers for years.

This phenomenon shows up in our data in what we are calling the vulnerability escape rate (VER). In the first two months of an application's tenure on the Contrast Application Security Platform, an average 12 vulnerabilities—six of them serious—occur in the software. But these numbers shrink steadily, reaching 6 total vulnerabilities and 3 serious in the ninth month. By the end of the first year, the average application sees no new serious vulnerabilities and just one non-serious one each month. This equates to a reduction of 50% in nine months and 92% in one year.

50%

reduction in the vulnerability escape rate (VER) in 9 months; 92% after 1 year

Faster Remediation, Lower Security Debt and Risk

This improvement in VER over time is one contributor to the fast vulnerability remediation timelines that Contrast customers achieve. Overall, they saw much better remediation timelines than organizations using legacy application security tools. The median time to remediate fixed vulnerabilities—that is, the time it took to resolve half of all closed vulnerabilities—was just three days in our dataset. This was nearly 29 times faster than the 86 days reported by a traditional static application security testing (SAST) vendor. Further, security debt gets paid down quickly, with nearly three-quarters (74%) of serious vulnerabilities remediated within 90 days and 90% of them within a year.

The result of this astounding remediation timeline is that organizations are reducing their per-application vulnerability backlog. Contrast customers saw continued improvement in the past year, shrinking the average number of vulnerabilities in an application to 21, down from 26 in the previous 12 months—a 19% decline.

Companies with lower-than-average security debt have an advantage when it comes to remediation time. Such organizations in our dataset achieved a median time to remediate all vulnerabilities of 2 days compared with 11 days for all organizations—an 82% improvement.

NEARLY 29X FASTER: 50% OF FIXED VULNERABILITIES CLOSED

3 days

Contrast Customers

86 days

Traditional SAST

SECURITY DEBT

21

Per Application: 21 vulnerabilities, down from 26

MEDIAN TIME TO REMEDIATE FOR ALL VULNERABILITIES

11

All Organizations: 11 days

2

Organizations With Smaller Than Average Security Debt: 2 days (82% less)

More Attacks, But Fewer are Viable

The typical organization was pummeled with 25,343 application attacks every month over the past year. But one of the biggest trends in the attack data is the percentage of attacks that were viable, which was cut in half—from 2% last year to 1% this year. A viable attack is one that hits an existing vulnerability within an application, and therefore has a chance of being successful. But non-viable attacks—sometimes referred to as probes—provide critical intelligence for cyber criminals that can inform a future successful attack. Eleven of the top 12 attack types impacted a larger share of applications this year than last year, with big increases in broken access control, SQL injection, cross-site scripting (XSS), command injection, and expression language (EL) injection.

25,343

Attacks per organization per month

1%

of attacks were viable, down from 2%

PERCENTAGE OF APPLICATIONS ATTACKED ROSE BY 9+ PERCENTAGE POINTS:

Broken Access Control, SQL Injection, XSS, Command Injection, EL Injection

Riskscores Headed Downward

The report also updates the Contrast RiskScore Index, a numerical score that helps organizations rank and visualize the risk posed by different vulnerability types over time. The five highest RiskScores were quite consistent over the entire 12 months, but the average RiskScore declined by more than 1.25 points over the course of a year. This is because our data comes from Contrast Security customers, whose risk level declines as they build tenure with the solution (viz., the number of vulnerabilities being introduced declines and overall security increases). Vulnerability types that saw especially big declines include four types of injection—SQL, hibernate, NoSQL, and expression language (EL).

Top 5 Riskscores (Annual Averages)

9.45

Broken Access Control

8.13

Cross-site Scripting

7.36

Insecure Configuration

7.07

SQL Injection

6.80

Sensitive Data Exposure

Takeaways

Findings in this report show that it is increasingly important for organizations to address software vulnerabilities in a timely manner, reduce their security debt, and prioritize their application security efforts according to actual risk. This is impossible to achieve without detailed observability on vulnerabilities, attacks, and open-source usage and security. Without it, organizations will not only waste scarce staff time on vulnerabilities that pose no risk but they may also defer action on truly dangerous issues in their software.

Instrumentation enables effective prioritization with continuous scanning, immediate feedback, and full observability. Contrast customers have a fuller understanding of which code is used by the software, which routes are exercised within the application, and what vulnerabilities need prioritized attention. The result is faster vulnerability remediation, reduced security debt, and fewer new vulnerabilities in applications.

Contrast Security provides the industry's most modern and comprehensive Application

Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

**240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133**



contrastsecurity.com