Contrast SECURITY

JULY–AUGUST 2020

Contrast Labs Application Security Intelligence Bimonthly Report

Table of contents

01 | Executive Summary

The Contrast Labs Application Security Intelligence Report for July–August 2020 analyzes composite data from Contrast Labs to update readers on vulnerability and attack trends as observed with applications covered by Contrast Assess and Contrast Protect. General findings include:

- **Serious vulnerabilities occurred in just over one-quarter of applications**—a significantly lower percentage than in May and June. But this is a reversion to the mean after this number spiked in May and June.
- **A larger percentage of overall vulnerabilities were serious**, with a 14% increase over May and June.
- **Attacks on .NET applications increased significantly**, with the number of attacks per applications per month growing by 42%.
- **Fewer attacks were viable**, with only 1% of attacks hitting an existing vulnerability. This suggests that a larger percentage of attacks were probes.

The July–August report debuts the Contrast RiskScore™, which measures on a scale of 1 to 10 the likelihood that a vulnerability type will occur compared with the likelihood that a specific vulnerability will be attacked. Broken access control tops the list, followed by SQL injection, and insecure configuration.

While workers are settling into new work-from-home processes, development teams face the pressure to move even faster to meet new business imperatives. At the same time, security teams have extra responsibilities in protecting a remote workforce while application attacks continue unabated. These converging trends could spell trouble for organizations that do not have a strategic focus on application security.

Key Findings

98% of applications had at least one vulnerability

27% of applications had a serious vulnerability—down by 22% from May–June

99% of applications had five or fewer serious vulnerabilities

32% of all vulnerabilities were serious—up by 14% from May–June

42% increase in attacks per month for .NET applications over May–June

100% of .NET applications were targeted by an SQL injection attack

1% of attacks were viable—that is, they hit an actual vulnerability in the software

02 | Getting Accustomed to "The New Normal"

Contrast Labs' Application Security Intelligence Reports are published on a bimonthly basis to provide an update on the status of application security and help development and security teams prioritize their efforts. The report is based on vulnerability and attack telemetry from customer applications using Contrast Assess, Contrast SCA, and Contrast Protect.

Contrast Labs analyzes this data regularly to determine the overall prevalence of vulnerabilities and attacks, the level of risk they introduce, and which types are most common in protected applications. The report also identifies a Watch List that can aid development, security, and operations teams as they refine their application security strategy. While two-month fluctuations are often not large, publishing the reports on a regular basis helps readers to identify trends.

After some glitches in the fast transition to a work-from-home economy driven by the COVID-19 pandemic, office workers in the U.S. and around the world settled into a "new normal" of working from home in July and August. For developers, perhaps the largest impact was the pressure to roll out applications at an even faster pace than before. A recent study found that a majority of developers said that digital transformation (63%), DevOps (52%), and cloud migration (52%) initiatives have increased in priority since the companies closed their offices.[1]

Yet as developers churn out new software, the state of application security remains concerning. One troubling sign is the amount of security debt that plagues many organizations. A Ponemon Institute study commissioned by IBM found that 42% of respondents whose company had suffered a breach attributed the cause to a known but unpatched security vulnerability.[2] This is because the average firm fails to patch 28% of vulnerabilities, resulting in a backlog of 57,000 cases. Even more, 57% of organizations have not determined which vulnerabilities are the riskiest—a process that is more complicated than just looking up a Common Vulnerability Scoring System (CVSS) number.[3] Given this state of affairs, it is not surprising that another study found that 82% of organizations experienced multiple exploitable attacks on vulnerabilities.[4]

At the same time, the identification of new vulnerabilities continued apace. While new entries in the Common Vulnerabilities and Exposures (CVE) database slowed slightly in the first half of the year, they are now returning to their prior pace.[5] Microsoft, which disclosed 150% more vulnerabilities in the first half of 2020 than in all of 2019, addressed 120 vulnerabilities in its August Patch Tuesday release.[6] And Facebook announced strict new vulnerability reporting and disclosure policies for third parties that use its platform, with the goal of cleaning up risky vulnerabilities more quickly.[7]

Cyber criminals also continue to mount attacks on these vulnerabilities, and their ability to work across jurisdictions makes it difficult to bring them to justice for their actions. Two alleged Chinese hackers were indicted in July for multiple crimes with victims around the world,[8] and two Iranian nationals were recently charged with using SQL injection in a years-long crime spree that compromised data from consumers, companies, and the U.S. government.[9]

The problem will only get worse without proactive action. Security teams now have the added responsibility of protecting company assets with millions of new remote workers—along with all their prior responsibilities. Developers, whose productivity has increased substantially in the past few years due to methodologies like Agile and DevOps, must now work even faster. It can be a recipe for a major, successful attack.

03 | Application Vulnerability Trends

FOR JULY–AUGUST 2020, CONTRAST LABS IDENTIFIED SEVERAL APPLICATION VULNERABILITY TRENDS FROM ANALYSIS OF ITS AGGREGATE DATA:

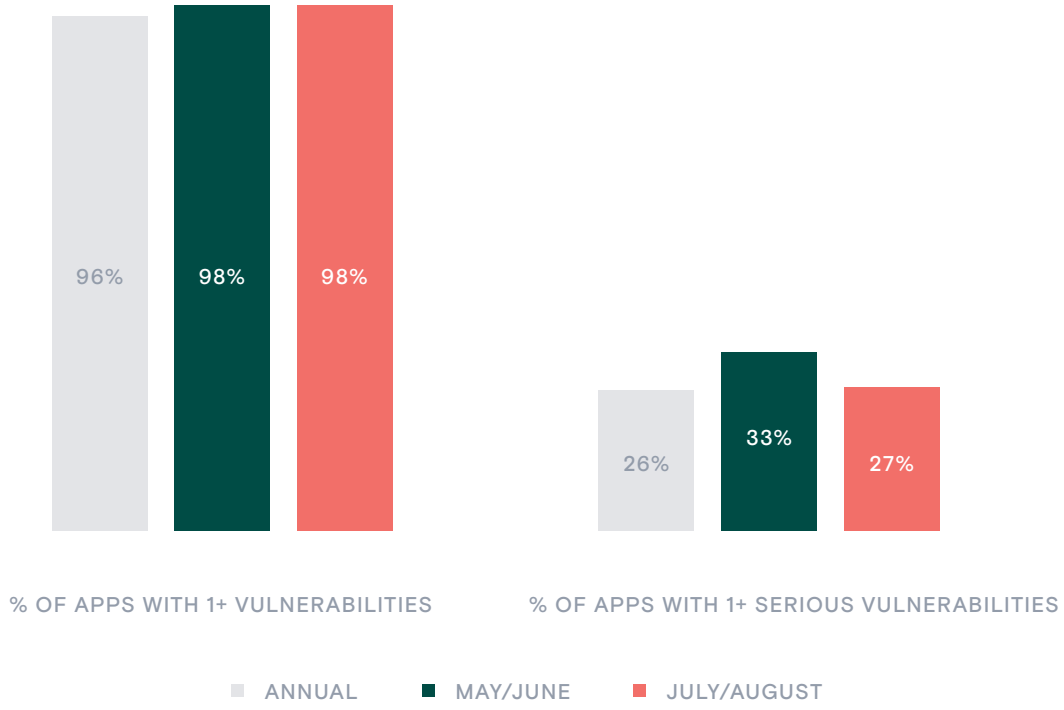
TREND: TOO MANY APPLICATIONS STILL HAVE VULNERABILITIES, BUT SERIOUS ONES WERE SLIGHTLY LESS WIDESPREAD

As has been the case with every Contrast Labs report, virtually every application in our dataset has some kind of vulnerability. The percentage of applications with at least one vulnerability stayed steady at 98% in July and August after reaching that peak in the prior two-month period (Figure 1). This number had crept up from the 96% reported for June 2019–May 2020 in Contrast's annual Application Security Observability Report.[10]

Some of these vulnerabilities, however, pose little risk to organizations. Serious vulnerabilities—those rated as "High" or "Critical"—were present in only 27% of applications. This percentage is down from 33% in May and June, though this reflects something of a reversion to the mean, as the annual rate for the 12 months ending in May of this year was 26%. Regardless, it is concerning to see serious vulnerabilities occurring between one-quarter and one-third of all applications.

FIGURE 1

Percentage of applications containing at least one vulnerability and at least one serious vulnerability, June 2019–May 2020, May–June 2020, and July–August 2020.

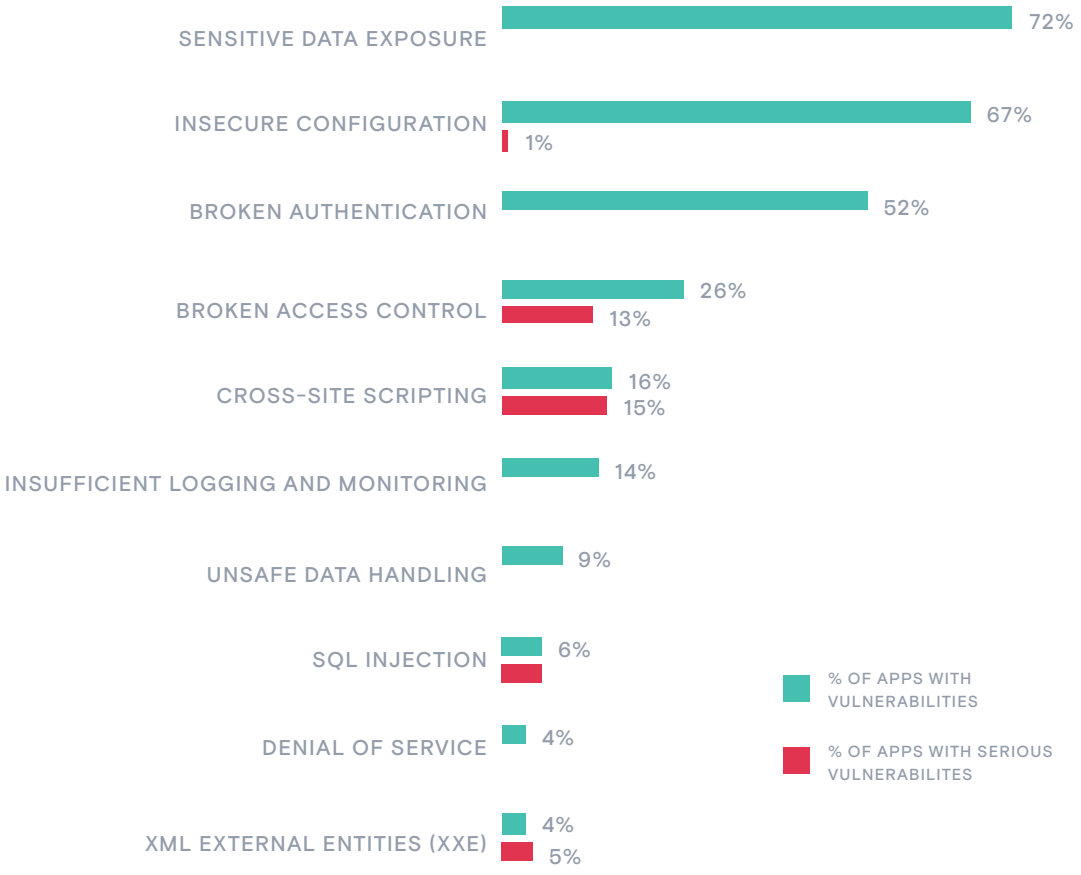


Analyzing overall vulnerabilities by category reveals that fewer applications contained several common vulnerability types compared with May and June (Figure 2). For example, applications containing XML external entities (XXE) injection vulnerabilities declined by 23%, cross-site scripting (XSS) went down by 18%, and insecure configuration was 17% less common. Nine other categories saw double-digit percentage decreases in prevalence among applications.

While this appears at first glance to be good news, a deeper look at the data shows that almost all these declines were in less risky vulnerabilities. Narrowing down the data to serious vulnerabilities only, virtually every category held very close to steady in terms of percentage of applications impacted. Two exceptions were serious insecure configurations, which impacted 60% more applications than in May and June (14% versus 9% in May–June) and serious insufficient logging and monitoring vulnerabilities, which impacted 25% fewer applications (26% compared with 33%).

FIGURE 2

Percentage of applications with vulnerabilities and serious vulnerabilities, select categories, July–August 2020.



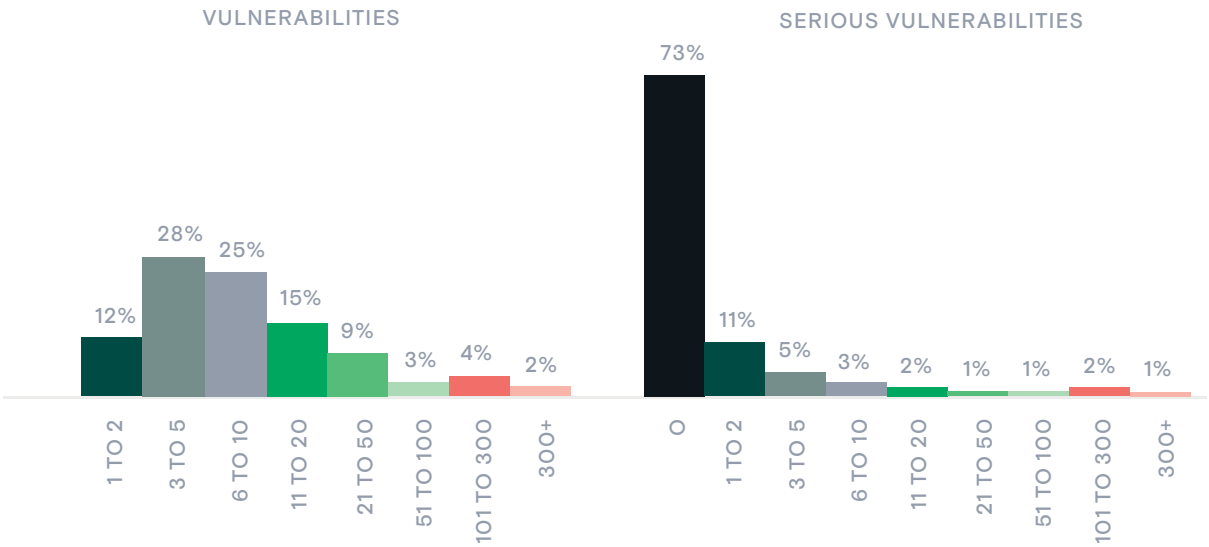
TREND: VULNERABILITIES PER APPLICATION TRENDED DOWNWARD, BUT A BIGGER PROPORTION OF VULNERABILITIES WERE SERIOUS

Overall vulnerabilities per application trended downward, with the percentage of applications reporting five or fewer vulnerabilities increasing from 31% to 42% between May–June and July–August—a 35% increase (Figure 3). However, this is a reversion to the mean, as the figure reported for the 12 months ending May 31 was that 50% of applications had fewer than five vulnerabilities.[11] Again, a likely explanation for the low number in May and June is the disruption of work rhythms in the second quarter due to new work-from-home processes.

The number of serious vulnerabilities per application also declined modestly, with the percentage of applications with five or fewer serious vulnerabilities increasing from 86% to 89%, and the percentage with no serious vulnerabilities improving from 67% to 73%—almost a 9% increase.

FIGURE 3

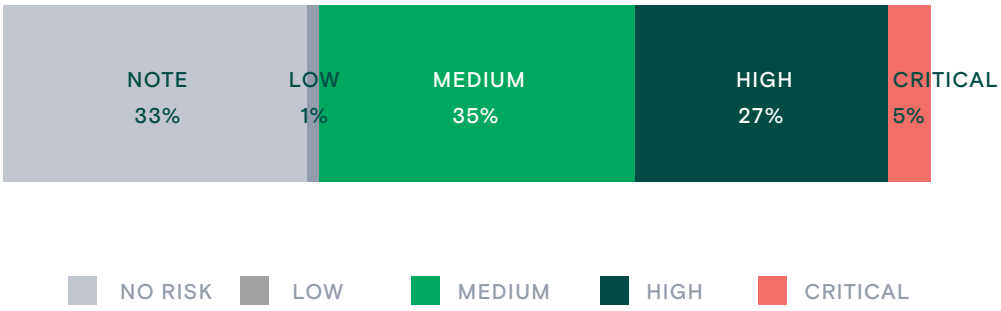
Percentage of applications with different numbers of vulnerabilities, July–August 2020.



While the percentage of applications with large numbers of serious vulnerabilities declined, the percentage of overall vulnerabilities that were serious went up. The percentage of overall vulnerabilities rated High or Critical went from 28% to 32%—a 14% increase. As we have seen above, declines in vulnerabilities are mostly attributed to less serious ones.

FIGURE 4

Percentage of vulnerabilities in each severity category, July–August 2020.



TREND: VULNERABILITIES REVERTED TO THE MEAN FOR .NET APPLICATIONS

Contrast Labs consistently finds more serious vulnerabilities in Java applications than in .NET applications, and July and August were no exception. Nearly 4 in 10 (39%) Java applications had at least one serious vulnerability, while only 17% of .NET applications had any (Figure 5).

The 17% result represents another reversion to the mean, as this dataset showed 29% of .NET applications had a serious vulnerability in May and June, but that figure was just 16% for the 12 months that ended on May 31.

Drilling down to categories reveals that the reduction in the percentage of .NET applications with a serious vulnerability is almost completely attributable to a reduction in the prevalence of serious XSS vulnerabilities—which were present in 10% of applications in July and August compared with 15% in the previous two-month period (Figure 6). All other categories for both languages were very consistent between the two periods.

FIGURE 5

Overall vulnerabilities in Java and .NET applications, July–August 2020.

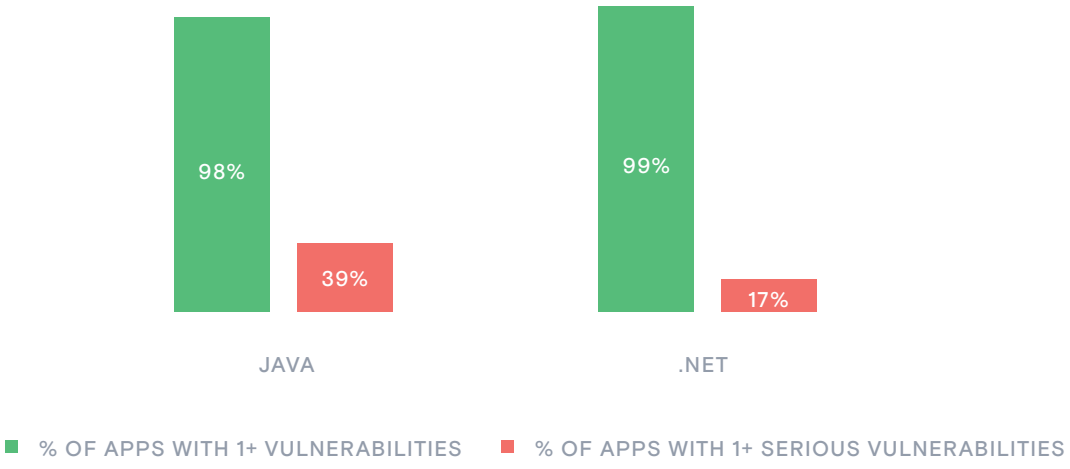
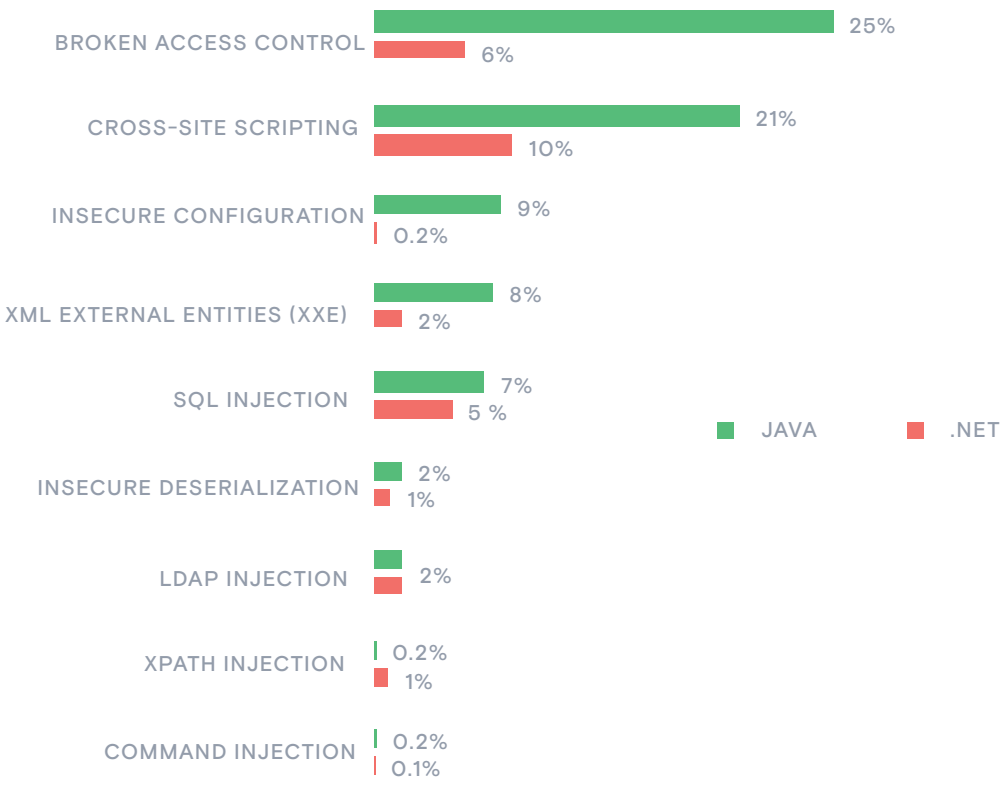


FIGURE 6

Vulnerabilities in Java and .NET applications by category, July–August 2020.



04 | Attack Trends

DATA FROM CONTRAST PROTECT DURING JULY AND AUGUST REVEALED A NUMBER OF TRENDS REGARDING ATTACKS:

TREND: OVERALL ATTACK VOLUMES DECLINED, BUT NOT FOR JAVA AND .NET

Monthly attacks per application continued to decrease: 8,346 in July and August compared with 9,008 in May and June and 13,279 for the 12 months ending May 31. However, this decline is completely driven by a sharp reduction in attack volume on applications using languages other than Java and .NET. Attack volumes were actually up for these common languages (Figure 7).

The good news is that the percentage of attacks that were viable—that is, that hit an actual vulnerability present in the software—declined. Only 1% of attacks were exploitable in July and August, compared with 3% in May and June and 2% for the 12-month period ending May 31 (Figure 8). Since attack volumes were up for the major programming languages, it may be that cyber criminals were sending an especially high number of probes in an effort to find vulnerabilities. The result would be reduced effectiveness for attacks overall.

FIGURE 7

Attacks per application per month for Java and .NET applications, July–August 2020.

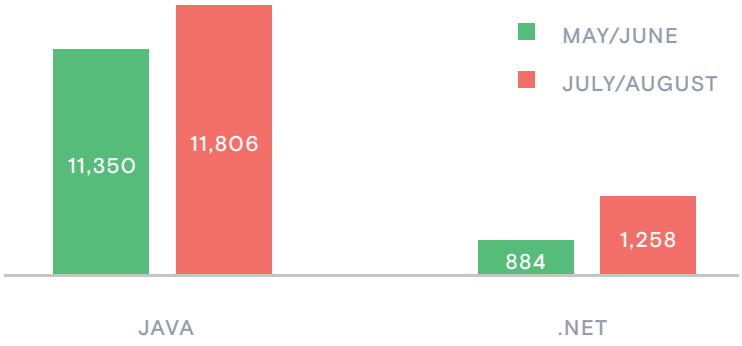


FIGURE 8

Percentage of attacks that were exploitable, by time period.

TREND: ATTACKS ON .NET APPLICATIONS INCREASED MUCH FASTER THAN ATTACKS ON JAVA APPLICATIONS

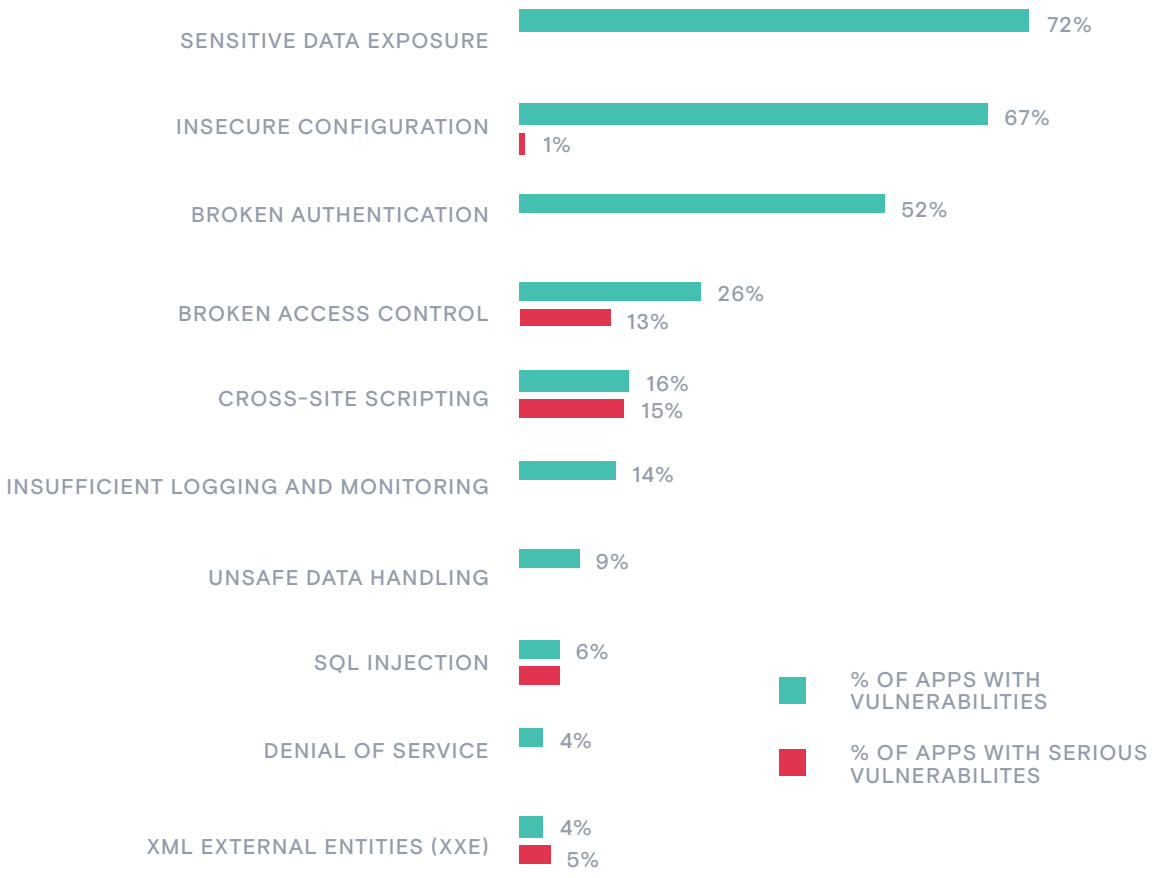
As noted, attack volumes increased in July and August for both Java and .NET applications, but the rise was not uniform. Compared with May and June, average attacks per application per month increased by a modest 4% for Java applications, though by an astounding 42% for .NET applications (Figure 7).

Of course, the increase in .NET attacks is from a much lower baseline, since our consistent finding is that .NET applications are much less frequently targeted than Java ones. The average number of monthly attacks on Java applications edged up from 11,350 to 11,806, while the increase for .NET was from 884 to 1,258. Nevertheless, this increase in attack frequency for .NET is concerning and should be monitored.

The increase in .NET attack volume may be partly driven by increases in the percentage of applications targeted by broken access control and SQL injection attacks (Figure 9). One hundred percent of .NET applications received an SQL injection attack in July or August, compared with 80% in May and June. More significantly, both numbers are significantly up from the average for the 12 months ending May 31, during which only 56% of applications received such an attack. Similarly, 71% of applications saw a broken access control attack compared with 56% in the annual average—although the number was at 80% in May and June.

FIGURE 9

Percentage of Java and .NET applications targeted by specific attack categories, July–August 2020.



05 | Contrast Riskscore Index

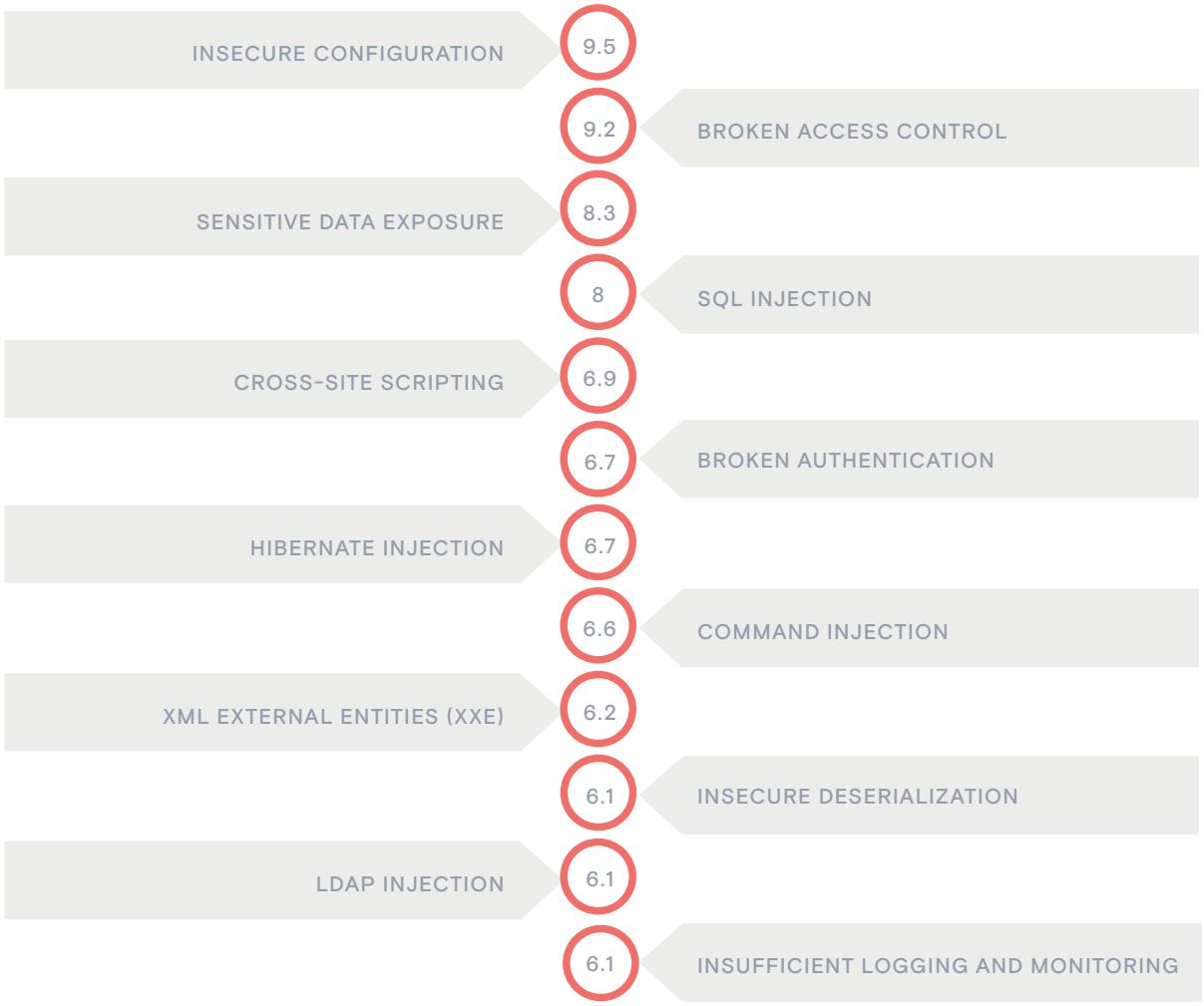
The vulnerability and attack data presented in this report provides important information for developers and security professionals as they work to ensure secure applications. But given the sheer number of vulnerabilities and attacks we report each time, how to prioritize the risk posed by each vulnerability and attempted attack is a crucial consideration. In the past, Contrast Labs compiled and published an Application Security Watch List for each bimonthly period. Seeking to further evolve this list, Contrast Labs developed a proprietary algorithm for calculating a RiskScore™ Index based on its continuous analysis of vulnerabilities and attack datasets. This bimonthly report is the first one to include it.

The ranking in the RiskScore Index is based on the likelihood that a vulnerability type will occur compared with the likelihood that a specific vulnerability will be attacked. The RiskScore Index for July and August of 2020 is detailed in Figure 10 while Figure 11 details the numbers from which the score is derived, the likelihood of a vulnerability, and the likelihood of an attack for each vulnerability type.

Insecure configuration took over the number one spot in the RiskScore Index in July–August. 67% of applications reported an insecure configuration vulnerability, with 4% having at least one serious insecure configuration vulnerability. This is up from the numbers in Contrast Labs' 2020 Application Security Observability Report where only 1% of applications had a serious insecure configuration vulnerability.

FIGURE 10

Top 12 vulnerability categories by Contrast RiskScore™ Index, July–August 2020.



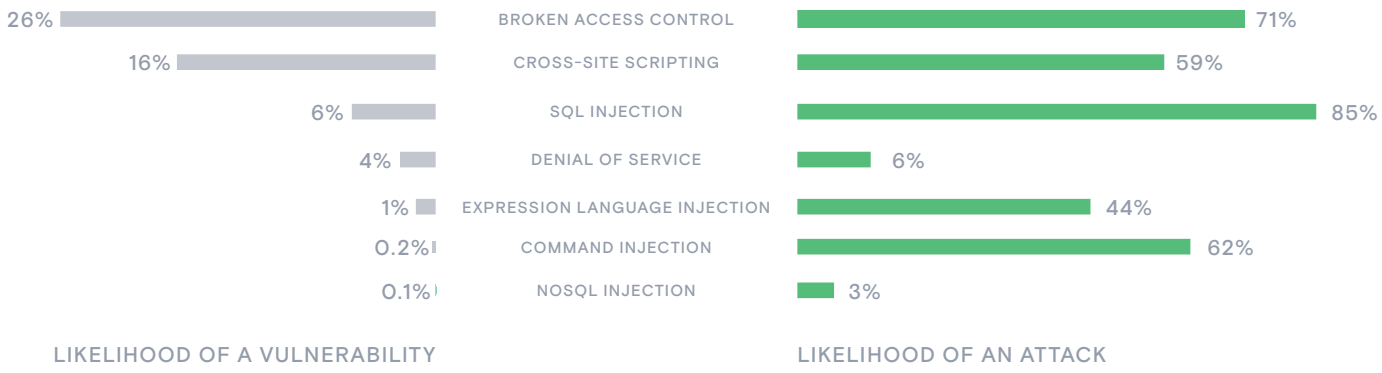
Broken access control remained the second highest vulnerability risk in July–August, with the percentage of applications vulnerable to such attacks increasing from 17% in May–June to 26% in July–August—a 53% increase.

SQL injection was the highest vulnerability risk in the May–June time frame. However, it moved down three spots to fourth for July–August. While relatively few applications (6%) were vulnerable to this attack type, 85% of all applications—and 100% of .NET applications—sustained this attack type (Figure 11). SQL injection attacks continue to make headlines, including the charging of two Iranian nationals who allegedly stole data from many private- and public-sector web applications.[12] Similarly, suspected Chinese hackers indicted in July used web-based attack techniques to install a webshell and use it to exfiltrate data.[13]

LDAP injection and hibernate injection rotate onto this list for this two-month period. While less likely than other variables on the list, both are serious injection vulnerabilities, with high impact scores, which teams should prioritize for remediation.

FIGURE 11

Likelihood of a vulnerability vs. likelihood of an attack, July–August 2020.



06 | Conclusion

Although operations at many companies may have felt more stable in July and August than in the several previous months, software vulnerabilities and attacks did not slow down significantly. While a few of the numbers in this report reverted to a more "normal" level after being anomalous in the first few months of the COVID-19 pandemic, these more customary figures are by no means optimistic.

Vulnerability telemetry indicates that more than one-quarter of applications still had at least one serious vulnerability in July and August, and 11% had more than five. While decreases in some vulnerability types appear at first glance to be good news, further analysis makes it clear that serious vulnerabilities in those categories have remained largely constant. Development teams may have stabilized their operations, but they have not yet improved their risk profile compared with the months leading up to the pandemic.

Similarly, a decrease in overall attack volumes is welcome, but more analysis shows that attacks on Java applications were actually more frequent—and the frequency of attacks on .NET applications surged by 42%. This makes it clear that applications using the two most common programming languages are even more targeted. And while only 1% of attacks were viable, the thousands of probes sent may provide information useful to cyber criminals in the future.

As with previous Contrast Labs bimonthly reports, the aggregate data in this report was gathered from enterprises using Contrast's instrumentation-based application security platform. It is hoped that readers will use the data presented here to structure and prioritize their application security efforts.

By embedding continuous security testing and runtime protection within the application itself, instrumentation enables application security observability from development through production. Such an approach enables vulnerabilities to be found and remediated much earlier in the software development life cycle (SDLC)—a process known as "shifting left."[14] At the same time, it allows organizations to "shift right" to protect applications in production.[15] The result is continuous, comprehensive protection throughout the SDLC.

Contrast SECURITY

[1] Veronica Haggar, "The Future of Remote Work and Software Development," DevOps.com, September 22, 2020.
[2] "The State of Vulnerability Management in the Cloud and On-Premises," Ponemon Institute and IBM, August 2020.
[3] Lisa Morgan, "Focused on application vulnerabilities? You're missing the bigger picture," SD Times, March 2, 2020.
[4] Based on a survey of 250 development, security, and operations professionals globally conducted by Contrast Security.
[5] "Vulnerability reporting is returning to normal," Help Net Security, August 28, 2020.
[6] Catalin Cimpanu, "Microsoft August 2020 Patch Tuesday fixes 120 vulnerabilities, two zero-days," ZDNet, August 11, 2020.
[7] Ionut Arghire, "Facebook Announces Vulnerability Reporting and Disclosure Policy," SecurityWeek, September 4, 2020.
[8] United States of America v. Li Xiaoyu and Dong Ziazhi, July 7, 2020.
[9] John Leyden, "Iranian cybercrime duo charged with multiple US hacking offenses," The Daily Swig, September 17, 2020.
[10] "Contrast 2020 Application Security Observability Report," Contrast Security, July 2020.
[11] "Contrast 2020 Application Security Observability Report," Contrast Security, July 2020.
[12] John Leyden, "Iranian cybercrime duo charged with multiple US hacking offenses," The Daily Swig, September 17, 2020.
[13] United States of America v. Li Xiaoyu and Dong Ziazhi, July 7, 2020.
[14] Jakob Pennington, "Shifting Left: DevSecOps as an Approach to Building Secure Applications," Medium, July 18, 2019.
[15] Alan Shimel, "DevOps Chat: Shifting Security Left and Right, With Contrast Security," Security Boulevard, October 7, 2019.

Contrast SECURITY

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

Contrast SECURITY

contrastsecurity.com