CONTRAST SECURITY

CONTRAST LABS APPLICATION SECURITY INTELLIGENCE BIMONTHLY REPORT

NOVEMBER–DECEMBER 2020

TABLE OF CONTENTS

01 | EXECUTIVE SUMMARY

The Contrast Labs Application Security Intelligence Report for November–December 2020 analyzes aggregate vulnerability and attack data from Contrast Security customers to help development, security, and operations teams to understand trends that can inform prioritization of application security efforts. This prioritization is especially important as organizations digest the impact of the massive SolarWinds breach, disclosed in mid-December, on thousands of organizations and the U.S. government.

Key findings include:

- **The percentage of applications that have at least one serious vulnerability increased again** to 33%, reflecting what is now a six-month trend. Serious insecure configurations were 10% more prevalent than in September–October.

- **More .NET applications continued to have serious vulnerabilities, while things improved with Java applications.** Only 36% of Java applications had such vulnerabilities, the lowest level in 10 months. But 24% of .NET applications were in that position, not far from an all-time high. As more organizations embrace .NET applications in development, these higher percentages will have a greater impact.

- **A higher percentage of attacks were probes as attackers search for ways to infiltrate** organizations. 99% of attacks in November–December did not hit an existing vulnerability, compared with 98% in September–October.

These findings highlight the risk posed by an increasing prevalence of serious vulnerabilities, something that must be addressed by moving beyond application security approaches that were designed for long-obsolete development methodologies. This is best accomplished by building testing and protection into every step of the software development life cycle (SDLC).

KEY FINDINGS

33% of applications have at least one serious vulnerability—up from 30% in September–October

9% of applications have 20+ serious vulnerabilities—down from 10% in September–October

58 average serious vulnerabilities in applications with at least one serious vulnerability—down from 56 in September–October

10% increase in prevalence of serious insecure configuration vulnerabilities from September–October—from 4% to 5% of applications

36% of Java applications have at least one serious vulnerability, lowest level in 10 months

24% of .NET applications have at least one serious vulnerability, up from 22% in September–October

99% of application attacks were probes that did not hit existing vulnerabilities—up from 98% in September–October

02 | MAJOR BREACH HIGHLIGHTS APPLICATION SECURITY DEFICIENCIES

Contrast Labs' bimonthly Application Security Intelligence Reports strive to provide a broad and accurate source of application threat intelligence for development, security, and operations teams that work to deliver more secure applications for their organizations. The reports highlight trends in both software vulnerabilities and application attacks based on telemetry data from applications using Contrast Assess during development and Contrast Protect in production. Contrast Labs provides regular analysis of this data to update readers on the level of risk posed by various kinds of vulnerabilities found in a wide range of applications.

While much of the press was preoccupied with the U.S. presidential election and its aftermath, a massive cyberattack on SolarWinds Inc. was disclosed in mid-December. Characterized by at least one analyst as among the worst breaches of the past decade[1], the attack gave the perpetrators advanced access[2] to the networks of more than 18,000 organizations[3] that use SolarWinds infrastructure software. Among them were multiple agencies of the U.S. federal government, including groups that manage top-secret information.[4]

The attackers compromised the SolarWinds software factory by altering its application code.[5] The attackers reportedly moved laterally within the SolarWinds network for several months before being discovered.[6] U.S. intelligence agencies attributed the attack on the Russian government in a joint statement in early January.[7]

The damage has yet to be fully assessed, but experts fear that the U.S. government breaches alone will be costly—financially and in their impact on national security.[8]

In other news, Mashable disclosed in November that an application attack resulted in the public posting of a database of personal user information.[9] And Her Majesty's Revenue and Customs (HMRC), the United Kingdom's tax collection agency, reported that 11 data breaches impacting more than 18,000 citizens occurred in the 2019-2020 financial year, prompting one law firm to brand their cybersecurity measures as "incompetent."[10]

These incidents and others highlight the grave risk posed when organizations fail to prioritize application security. Cyber criminals and malicious nation-states are increasingly using applications as the vector to attack corporate and government networks. One recent study by the Ponemon Institute and IBM found that 42% of organizations that suffered a breach attributed the cause to a *known but unpatched* software vulnerability.[11]

03 | APPLICATION VULNERABILITY TRENDS

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

TREND: SERIOUS VULNERABILITIES CONTINUE TO IMPACT MORE APPLICATIONS

The share of applications containing at least one serious vulnerability (Critical or High severity) continued to edge upward, with 32% impacted by such vulnerabilities in November and December (Figure 1). This is the highest percentage recorded since May and June of last year. It is also significantly more than the 26% reported in the mostly pre-pandemic annual average published in the 2020 Contrast Labs Application Security Observability Report, covering the 12 months ending May 31, 2020. A total of 97% of applications had at least one vulnerability of some sort, consistent with findings over the past 18 months.

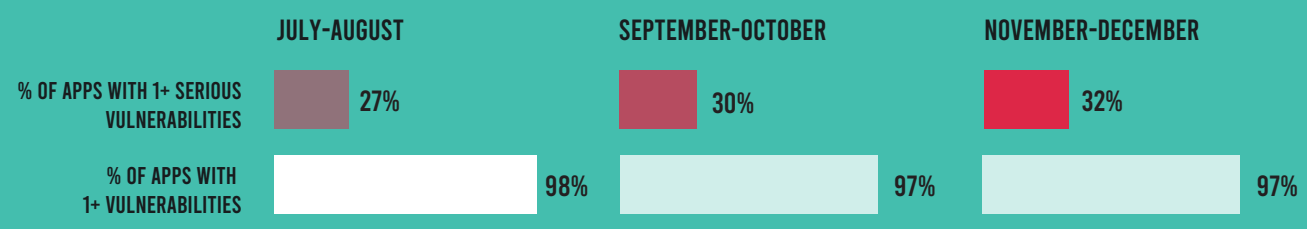


Figure 1: Percentage of applications containing at least one vulnerability and at least one serious vulnerability, three bimonthly periods.

Drilling down to vulnerability type, it is notable that the percentage of applications impacted by serious insecure configurations was up 10%, from just over 4% to just under 5% (Figure 2). And the share of applications containing serious XML external entities (XXE) vulnerabilities increased by 8%. On the other hand, serious SQL injection vulnerabilities were found in 7% fewer applications than in September–October.

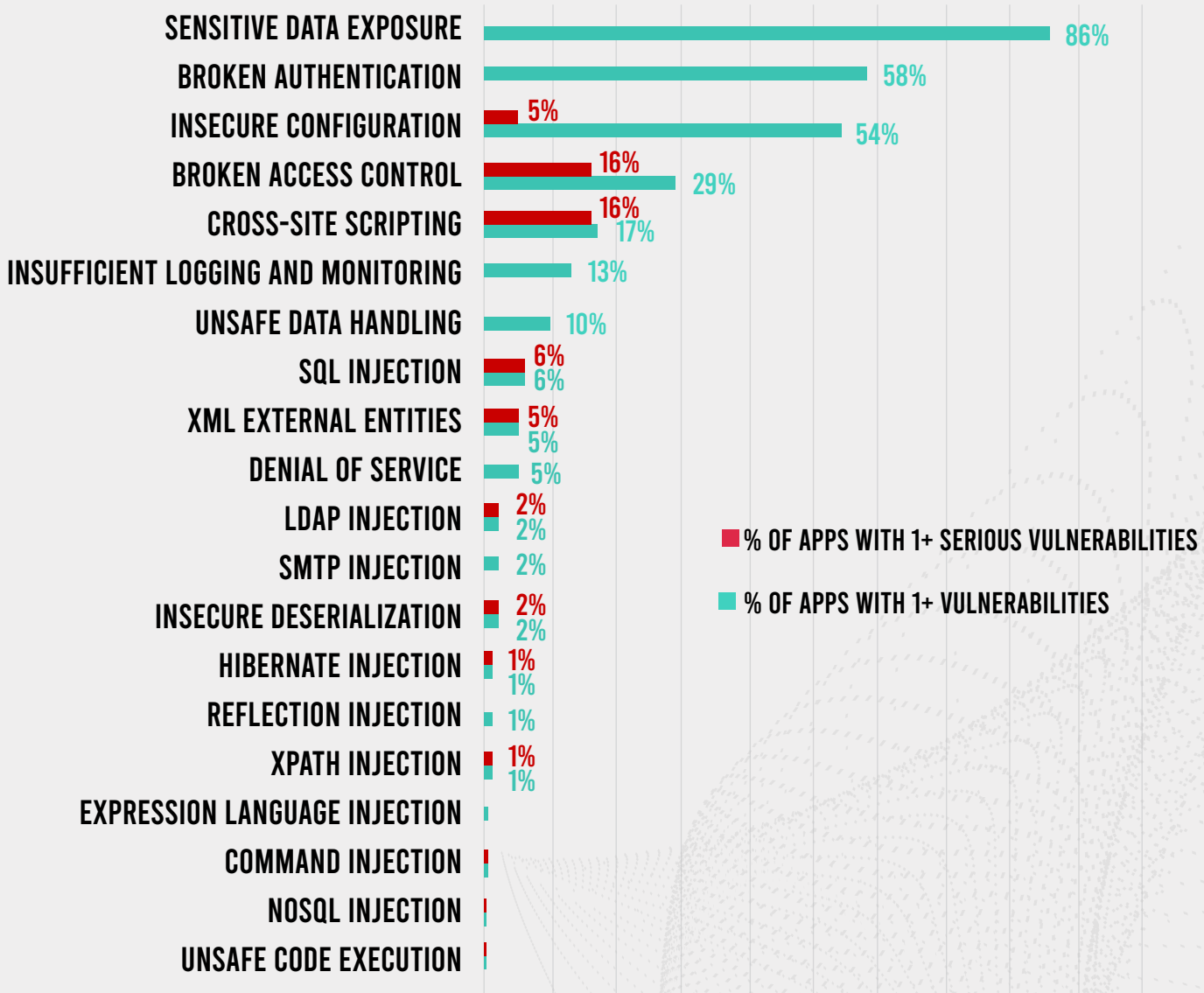


Figure 2: Percentage of applications with vulnerabilities and serious vulnerabilities, by category, November–December 2020.

TREND: THE PERCENTAGE OF VULNERABILITIES THAT ARE SERIOUS REMAINED HIGH

The percentage of all vulnerabilities that were serious remained steady at 33%, with no change from September–October (Figure 3). However, the percentage that were rated Critical as opposed to High decreased slightly, to 4% of vulnerabilities. While this figure was unchanged from the last bimonthly report, it is up from earlier in the year.

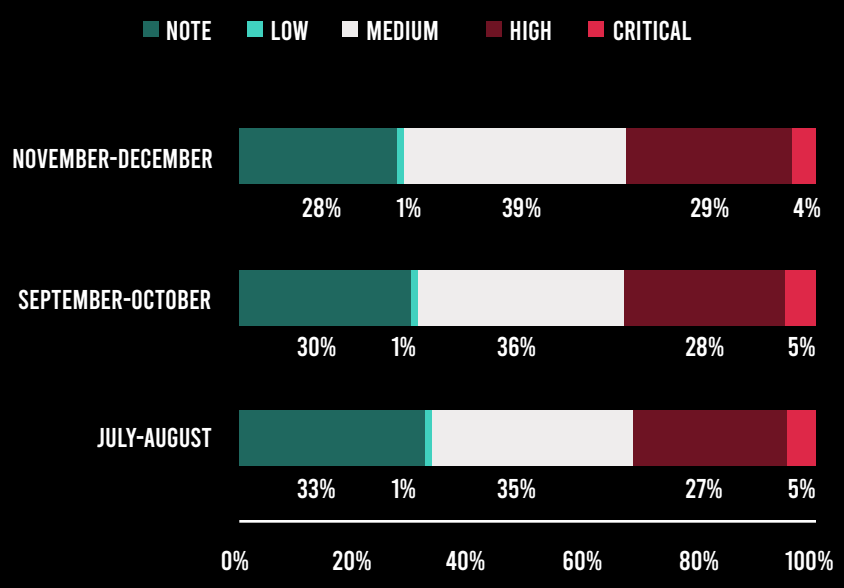
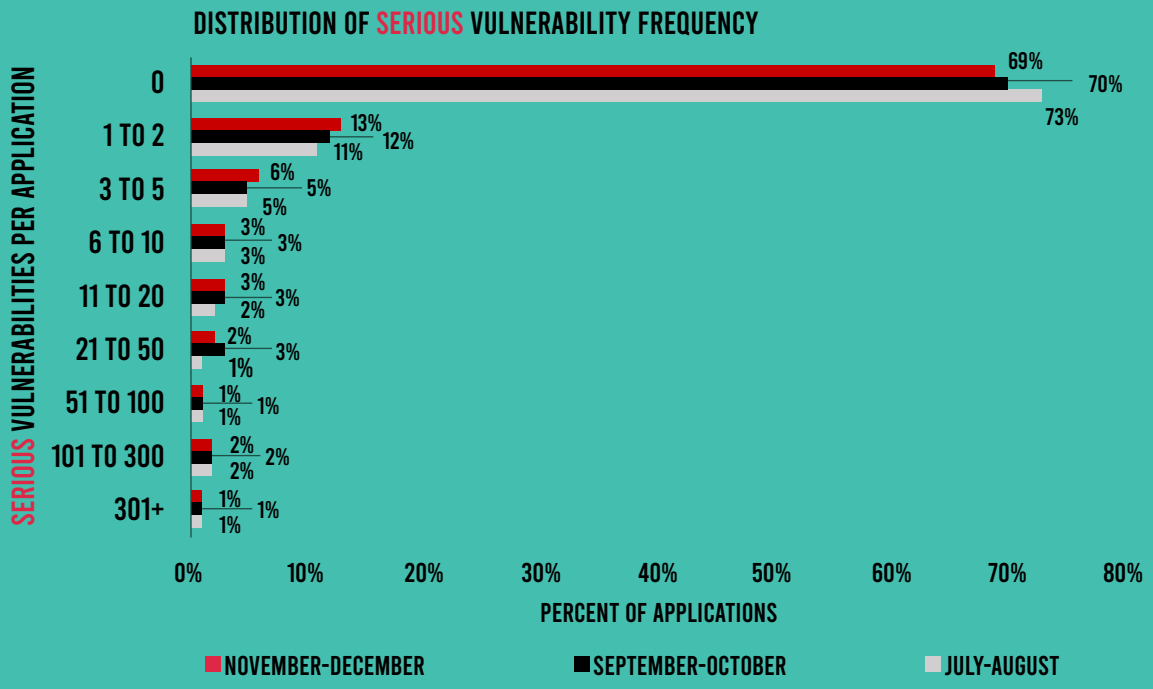


Figure 3: Overall vulnerabilities by severity, three bimonthly periods.

One piece of good news: Fewer applications have more than 50 vulnerabilities—9% in November–December versus 11% in September–October (Figure 4). The share of applications with more than 20 serious vulnerabilities also declined, from 7% to 6%. This brings these two statistics more in line with longstanding averages, though far too many applications still have large numbers of serious vulnerabilities.



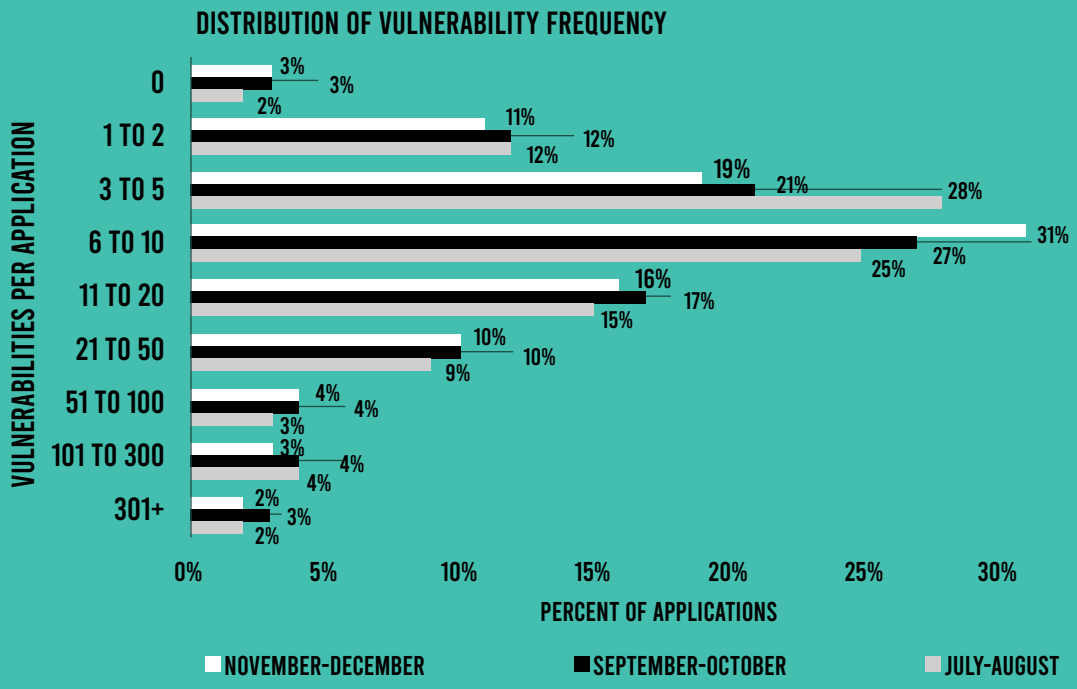


Figure 4: Vulnerabilities and serious vulnerabilities per vulnerable application over three bimonthly periods.

A similar downturn occurred in the average number of serious vulnerabilities found in the subset of applications that contain at least one serious vulnerability, which declined from 60 to 58 between September–October and November–December (Figure 5). Again, this move reflects a reversion to the mean, as this number hovered near 55 from March through August. Regardless, such a high number of serious vulnerabilities is risky for any application, let alone an average vulnerable application.

Figure 5. Average number of vulnerabilities and serious vulnerabilities per vulnerable application over three bimonthly periods.

TREND: FEWER JAVA APPLICATIONS—AND MORE .NET APPLICATIONS—HAD SERIOUS VULNERABILITIES

Looking at vulnerability data by programming language, Java and .NET applications saw trends heading in opposite directions. Only 36% of Java applications had at least one serious vulnerability, the lowest level in 10 months and significantly below the annual average of 42% for the period ending on May 31 (Figure 6). Not surprisingly, the percentage of Java applications containing each of the top five vulnerability types declined by between 9% and 16% compared with September–October (Figure 7).

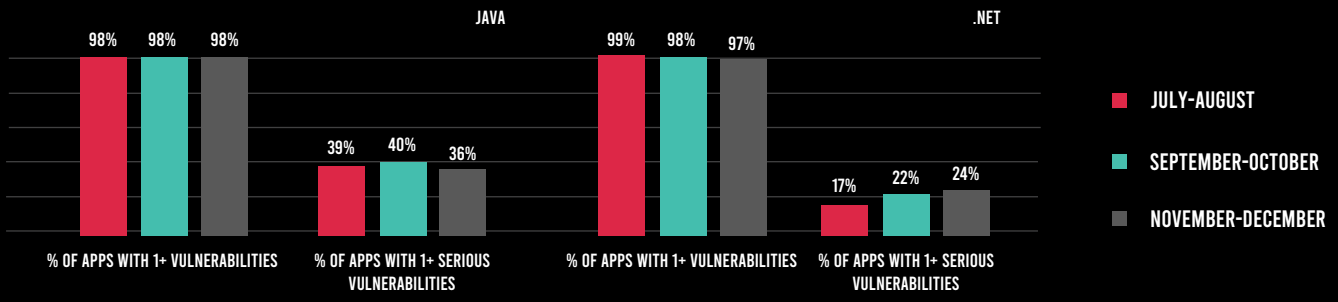


Figure 6. Overall vulnerabilities and serious vulnerabilities in Java and .NET applications over three bimonthly periods

On the other hand, 24% of .NET applications contained at least one serious vulnerability, up from 22% in September–October and 16% for the mostly pre-pandemic annual average (Figure 6). Similarly, four of the top five vulnerability types increased in prevalence compared with September–October (Figure 7). Notably, 8% more .NET applications had serious cross-site scripting (XSS) vulnerabilities than in the prior bimonthly period. While it is still true that fewer .NET applications have serious vulnerabilities than Java ones, the gap has been steadily closing in recent months.

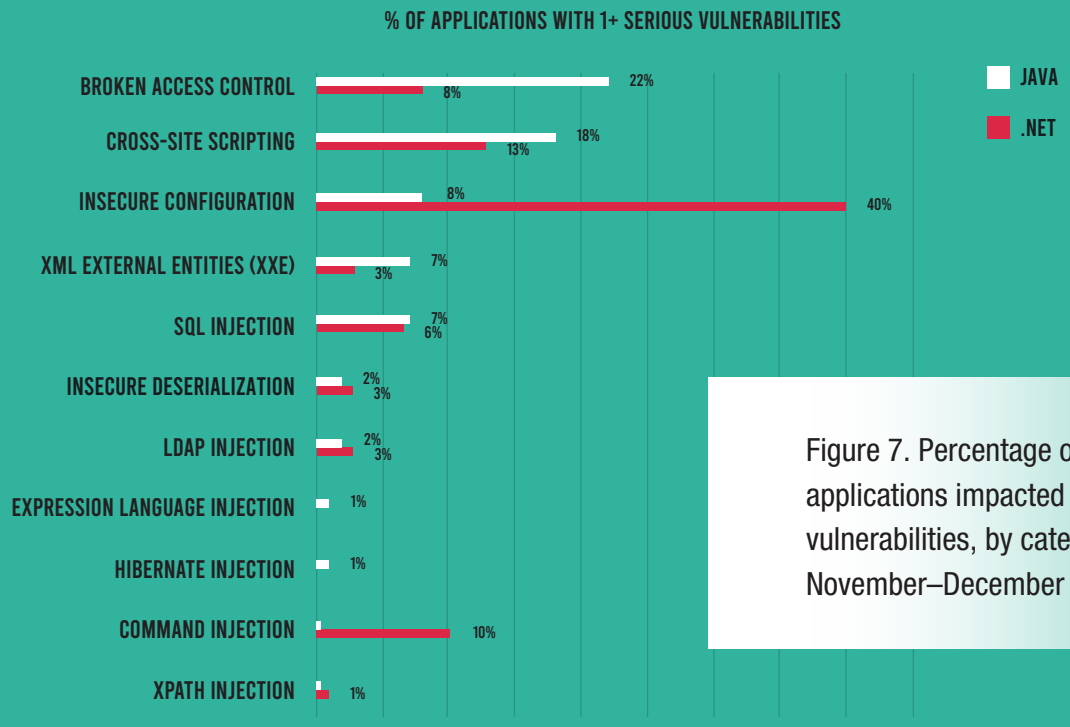


Figure 7. Percentage of Java and .NET applications impacted by serious vulnerabilities, by category, November–December 2020.

04 | ATTACK TRENDS

DATA FROM CONTRAST PROTECT DURING NOVEMBER AND DECEMBER REVEALED SEVERAL TRENDS REGARDING APPLICATION ATTACKS:

TREND: MORE ATTACKS WERE PROBES, AND THE TOP ATTACK TYPES ARE TRENDING UPWARD OVER TIME

The percentage of attacks that were viable—that is, hit a vulnerability that was present in the application targeted—went back down to 1% after averaging 2% before the pandemic and hitting 2% or 3% several times since then (Figure 8). This means that 99% of attacks in November and December were probes as adversaries look for attack vectors that can be successful.

While the fact that 99% of attacks are harmless can be comforting, the 1% of attacks that hit existing vulnerabilities can still be significant given the thousands of attacks that applications sustain each month.

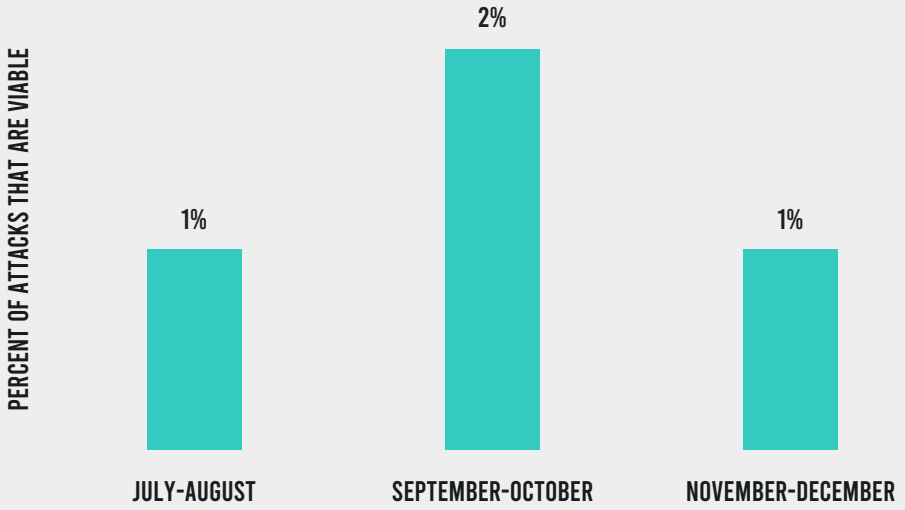


Figure 8. Percentage of attacks viable, three bimonthly periods.

Looking at the percentage of applications impacted, the top three attack types (broken access control, SQL injection, and XSS) remained relatively steady from the last report (Figure 9). However, OS command injection and EL injection declined significantly. But all five are up significantly compared with the 12-month average that ended in June 2020, encompassing mostly pre-pandemic times.

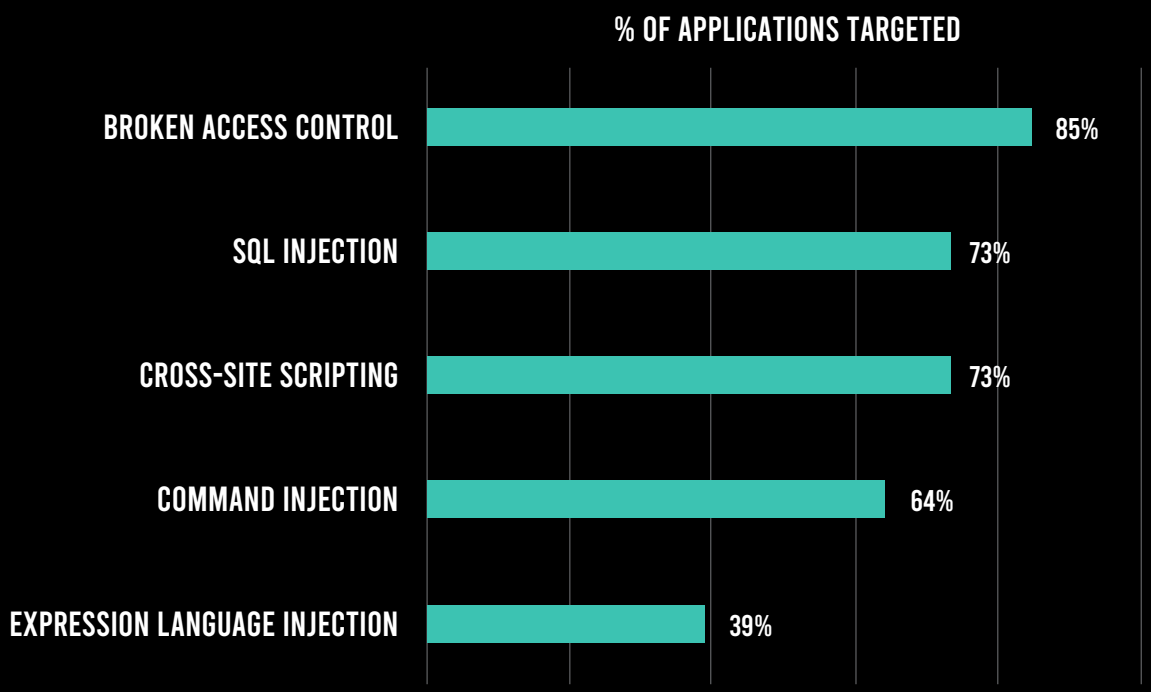


Figure 9. Percentage of applications targeted by the top five attack categories, November–December 2020.

TREND: SEVERAL TYPES OF JAVA ATTACKS DECLINED, WHILE TOP .NET ATTACK TYPES HELD STEADY

Looking at attacks by programming language, several attack types were less prevalent among Java applications than in September–October (Figure 10). The percentage of Java applications impacted by expression language (EL) injection and unsafe file upload attacks declined by 50% and 43%, for example. SQL injection attacks impacted just 75% of Java applications in November–December after targeting 90% of those applications in the prior bimonthly period. On the other hand, broken access control attacks impacted 94% of Java applications in November–December—a number that has steadily risen over the past year.

While there was a fair amount of fluctuation in attack types with Java applications, the numbers for .NET applications changed very little, with nearly every application sustaining SQL injection and OS command injection attacks and two-thirds sustaining XSS, EL injection, and unsafe file upload attacks.

Figure 10: Percentage of applications targeted by language and attack type over three bimonthly periods.

05 | CONTRAST RISKSCORE INDEX FOR NOVEMBER–DECEMBER 2020

In addition to the vulnerability and attack data presented in this report, Contrast Labs has developed an objective way to rank and visualize the relative risk presented by different vulnerability types over time, using a numerical score. Dubbed the Contrast RiskScore Index, its underlying algorithm embraces and extends industry-standard risk metrics with factors measured during both development and production. The November–December report is the first Application Security Intelligence Report to use the newly released beta version 0.5 for its calculations.[12] Plans are being executed to release the Contrast RiskScore Index later this year as an open-source tool that can be used to measure risk at an organizational level.

Broken access control remained the most dangerous vulnerability type, with a RiskScore of 9.68, slightly up from the last bimonthly period (Figure 12). XSS remained in the number two position despite a slight decline in its numerical score. Beyond these top two, there was significant churn in both rankings and numerical scores.

SQL injection moved from fifth place to third despite its RiskScore being almost level compared with September–October. Rather, the move in its ranking is the result of the RiskScores for other vulnerability types going down. Several other top vulnerability types saw significant fluctuation in numerical scores. Hibernate injection moved into the top five from seventh position in September–October, with a

three-quarters point increase to 6.4. Sensitive data exposure moved from 12th position to sixth, as its RiskScore increased by nearly two points. Insecure configuration remained in fourth position, but its RiskScore declined by more than a point and a half. And NoSQL injection, which had been increasing in RiskScore earlier in the year, declined by well over two points and moved from third position to seventh.

Figure 11. Top 10 vulnerability categories by Contrast RiskScore, July–December 2020.

06 | CONCLUSION

As applications become increasingly important in delivering value to rapidly evolving customer preferences in a variety of industries, the pressure to increase velocity continues to mount. This includes major additions and refinements to existing applications and development of new applications from scratch.

The SolarWinds attack is a wakeup call to organizations that they should shore up the security of their "software factory." All too often, the application security team operates largely outside this factory, making it impossible for them to deliver secure software via the processes—and the operational efficiencies—that the factory approach has enabled over time. The acceleration of digital transformation in 2020 has made this state of affairs completely unsustainable, and organizations have no choice but to integrate security into DevOps in 2021.

Telemetry from actual applications in November–December 2020 revealed several disturbing trends, including an increased percentage of applications impacted by serious vulnerabilities—an increase that was especially pronounced with .NET applications. And while fewer applications had as many as 50 vulnerabilities or 20 serious vulnerabilities, far too many pieces of software still hold that distinction.

Not surprisingly, application attacks continued unabated. Although a higher percentage of attacks were harmless probes in November–December than in September–October, this only means that attackers will use this information to narrow down their attack options in the future to more successful approaches.

Contrast Labs hopes that the findings presented here help readers prioritize their short-term application security efforts and refine their longer-term strategic plans. As government agencies and private businesses recover from the SolarWinds breach—and non-victims reassess their risk—moving beyond legacy approaches to application security will be an essential part of protecting organizations against similar future attacks. Custom code must be secure, open-source software must be free of known vulnerabilities, and applications must be protected in runtime.

Security instrumentation embeds continuous security testing and runtime protection within applications themselves, enabling application security observability throughout the SDLC. The result is that organizations can discover and repair vulnerabilities in near real time, rather than identifying them later in the process. This "shift left" enables developers to remediate problems as they go and prevents coding delays in the future.[13] Instrumentation also enables companies to "shift right" to protect applications in production as new vulnerabilities are identified.[14] This comprehensive and continuous protection helps organizations move beyond legacy application security approaches to methods that fit today's rapid

---

1 Michael Novinson, "SolarWinds Hack 'One Of The Worst In The Last Decade': Analyst," CRN, December 17, 2020.
2 Jason Lemon, "SolarWinds Breach Potentially Gave Hackers 'God Access': Ex-White House Official," Newsweek, December 16, 2020.
3 Michael Riley, et al., "Russia-Linked SolarWinds Hack Snags Widening List of Victims," Bloomberg, December 17, 2020.
4 Zachary Cohen, et al., "Massive hack of US government launches search for answers as Russia named top suspect," CNN, December 16, 2020.
5 Erik Costlow, "SolarWinds Hack Exposes Long Overdue Prioritization of Software Security," Contrast Security, December 22, 2020.
6 Josephine Wolff, "The SolarWinds Hack Is Unlike Anything We Have Ever Seen Before," Slate, December 18, 2020.
7 Laura Hautala, "SolarWinds software used in multiple hacking attacks: What you need to know," CNET, February 3, 2021.
8 Jason Miller, "SolarWinds incident should be a catalyst to rethink federal cybersecurity," Federal News Network, December 21, 2020.
9 "Notice of data security incident," Mashable, November 8, 2020.
10 Keumars Afifi-Sabet, "HMRC branded 'incompetent' following 11 serious data breaches," ITPro, December 7, 2020.
11 "The State of Vulnerability Management in the Cloud and On-Premises," Ponemon Institute and IBM, August 2020.
12 See "RiskScore Index Report," Contrast Security, February 2021.
13 Jakob Pennington, "Shifting Left: DevSecOps as an Approach to Building Secure Applications," Medium, July 18, 2019.
14 Alan Shimel, "DevOps Chat: Shifting Security Left and Right, With Contrast Security," Security Boulevard, October 7, 2019.

CONTRAST SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.