Contrast SECURITY

JANUARY–FEBRUARY 2021

Contrast Labs Application Security Intelligence Bimonthly report

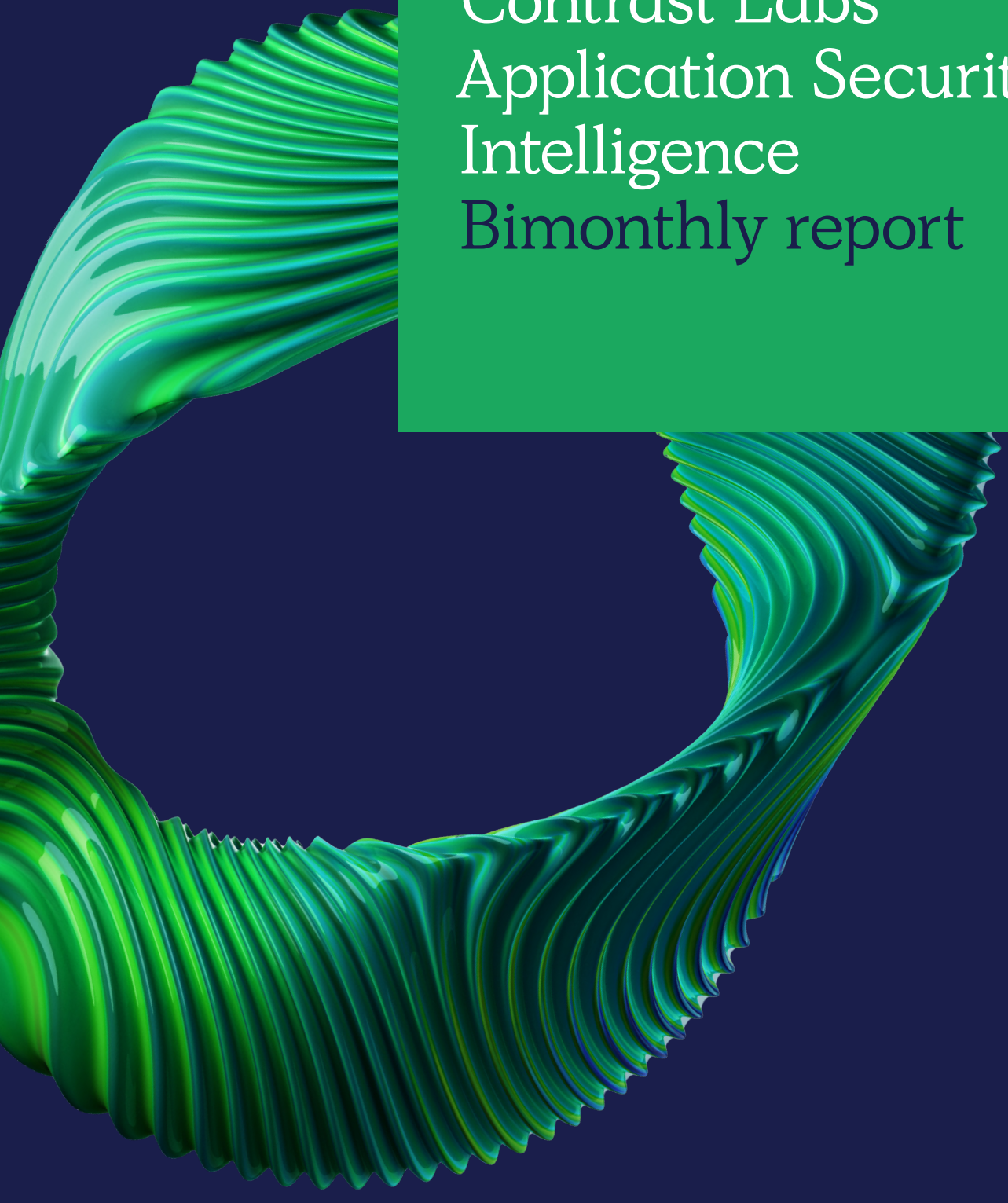


Table of contents

01 Executive Summary

01 | Executive Summary

The Contrast Labs Application Security Intelligence Report for January–February 2021 is based on aggregate vulnerability and attack data for custom code from Contrast Security customers. Its purpose is to help inform the prioritization of application security efforts by highlighting trends in both vulnerabilities and attacks. As applications become a more popular attack vector for cyber criminals, this intelligence is increasingly important to organizations' overall IT security.

Key findings include:

- **The percentage of applications with one or more serious vulnerabilities increased again** to 34%, a continuation of an eight-month trend. This includes an increased share of both Java and .NET applications.
- **A larger share of all vulnerabilities were rated as High or Critical**—39% compared with 33% in the prior bimonthly period—an 18% increase. This means that more vulnerabilities are high on the priority list for remediation for strapped security teams.
- **An exceedingly high percentage of attacks were probes**, with less than 0.5% of attacks hitting an existing vulnerability. While this is short-term good news, it also gives attackers more intelligence to use in the future. It also is a reminder that probes comprise the vast majority of threats; used by cyber criminals to probe for vulnerabilities across applications and application programming interfaces (APIs) and not actual attacks on vulnerabilities that can be exploited.

These findings reiterate the difficulty of creating software factories and supply chains that effectively prevent vulnerabilities from reaching production and being exploited. Application security tools and practices that were designed for the development methodologies of the past simply cannot scale to today's rapid and efficient software factory.

KEY FINDINGS

VULNERABILITY TRENDS

34%

of applications have at least one serious vulnerability—up from 32% in November–December and 27% in July–August

39%

of all vulnerabilities are Critical or High—up from 33% in November–December

39%

of Java applications and 28% of .NET applications have at least one serious vulnerability

ATTACK TRENDS

99%+

of all attacks in January–February were probes

89.5%

of attacks were broken access control or SQL injection

KEY FINDINGS

VULNERABILITY TRENDS

34%

of applications have at least one serious vulnerability—up from 32% in November–December and 27% in July–August

39%

of all vulnerabilities are Critical or High—up from 33% in November–December

39%

of Java applications and 28% of .NET applications have at least one serious vulnerability

ATTACK TRENDS

99%+

of all attacks in January–February were probes

89.5%

of attacks were broken access control or SQL injection

TOP 5 CONTRAST RISKSCORE™

9.11	BROKEN ACCESS CONTROL
8.89	CROSS-SITE SCRIPTING
6.72	INSECURE CONFIGURATION
6.60	SENSITIVE DATA EXPOSURE
5.85	SQL INJECTION

Contrast SECURITY

02 More Security Concerns for the Software Supply Chain

02 | More Security Concerns for the Software Supply Chain

Contrast Labs' bimonthly Application Security Intelligence Reports aim to help development and security teams prioritize their application security applications to deliver more secure applications for customers and co-workers. Every two months, we 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' analysis helps readers understand the evolving risk posed by different kinds of vulnerabilities.

As assessments continued on the damage caused by the massive SolarWinds attack that was revealed in December, news of attacks on Microsoft Exchange Server on-premises software using several zero-day exploits began to emerge in January.[1] Security researchers reportedly discovered the vulnerabilities in early January, but they had not yet been publicized when bad actors began exploiting them to gain access to email accounts. Patches were issued in early March, and all organizations are urged to apply them as soon as possible.[2]

In February, another security researcher discovered a new vulnerability type called dependency confusion and successfully pushed malicious proof-of-concept (POC) code to internal development builds at more than 35 technology companies.[3] Other researchers replicated this with other applications,[4] and cyber criminals began exploiting dependency confusion in attacks on organizations.[5]

Meanwhile, a zero-day vulnerability in SonicWall security products was exploited in the wild,[6] Amazon Kindle devices were targeted by the KindleDrip remote code execution attack,[7] and multiple additional vulnerabilities have been discovered in SolarWinds Orion software.[8]

These incidents are reminders that the software supply chain is under attack from all directions. Users of off-the-shelf applications can be victimized by attacks on software they have no control over. Developers that use third-party libraries and developer tools now have another attack vector to be wary of in dependency confusion. And as we will elaborate in this report, serious vulnerabilities in custom code are becoming more common. It is important for organizations to lock down all of these aspects of the software supply chain.

03 Contrast Riskscore for January–February 2021

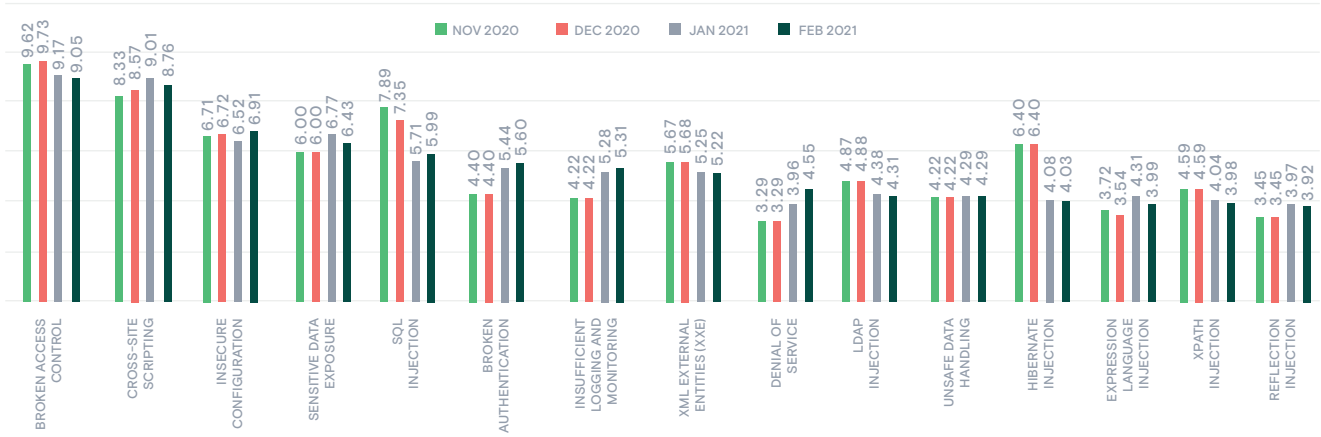
03 | Contrast Riskscore for January–February 2021

As described in a recent report,[9] Contrast Labs has developed a numerical score that provides an objective way to rank and visualize the relative risk presented by different vulnerability types over time. The underlying algorithm of Contrast RiskScore is regularly refined by Contrast Labs to improve its accuracy. Universal RiskScores such as those in this report are useful to security and development teams as they prioritize their application security activities. To add even more value, Contrast Labs has an open-source version of RiskScore in the works that will be available soon. This will enable measurement or risk at the organizational level—or even by individual application.

Broken access control and cross-site scripting (XSS) continue to top the RiskScore rankings (Figure 1). Broken access control has scored above 9 for each of the past 12 months, and XSS has scored over 8 in the same period. Nearly two full points separate the second- and third-highest scores. That third position now belongs to insecure configuration, which has been trending upward for several months, pushing sensitive data exposure to fourth position. SQL injection is in fifth position and is trending upward after a steep decline in its RiskScore late last year.

FIGURE 1

Top 15 vulnerability categories by Contrast RiskScore, November 2020–February 2021.



Further down the list, several major moves in RiskScores are interesting to note. Broken authentication is now in sixth position after increasing from 4.4 to 5.6 over four months. Hibernate injection remained near a RiskScore of 4 after seeing its score drop by more than two points between September–October and November–December of last year. And denial of service has been steadily increasing for eight months now, moving into ninth position in the RiskScore rankings.

FIGURE 2

Top 5 vulnerability categories by Contrast RiskScore, July 2020–February 2021.

04 Application Vulnerability Trends

04 | Application Vulnerability Trends

RiskScores are based on the vulnerability and attack trends noted through analysis of Contrast Labs' aggregate telemetry data. Readers seeking insight on vulnerabilities and attacks on third-party libraries can read the recent 2021 State of Open-source Security Report from Contrast Labs.[10] For custom code, Contrast Labs noted the following application vulnerability trends during January–February 2021:

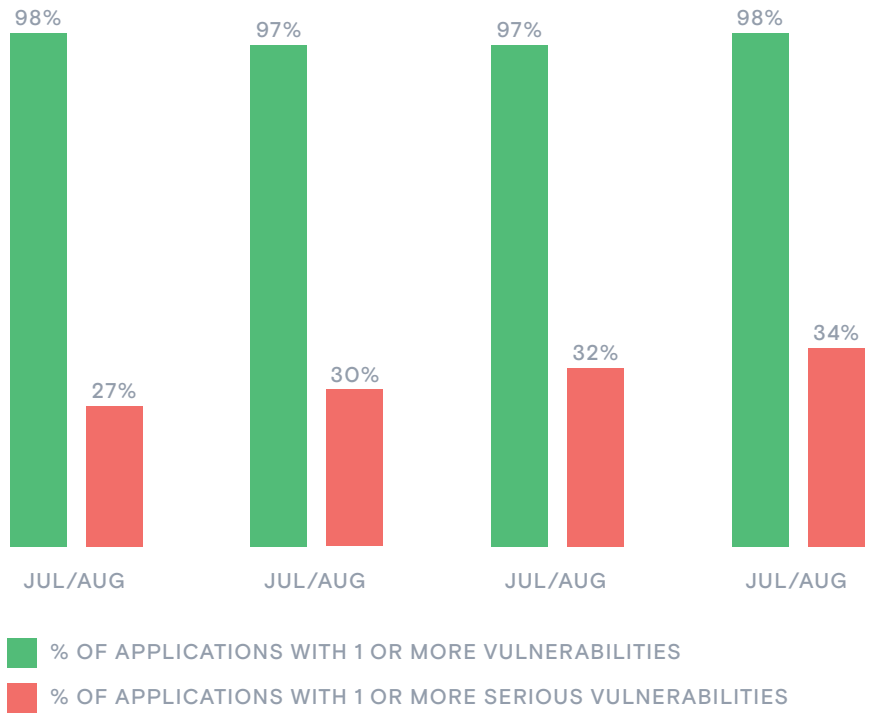
TREND: THE PERCENTAGE OF APPLICATIONS WITH SERIOUS VULNERABILITIES CONTINUES TO GROW

In our four most recent bimonthly reports, the percentage of applications that contain at least one serious vulnerability has steadily grown, from 27% in July–August of last year to 34% in January–February of this year (Figure 3). While almost every application continues to have some sort of vulnerability—and some vulnerabilities pose little or no risk to an organization—the fact that so many more applications have a serious one is a concern.

Looking at vulnerabilities by category, serious insecure configuration vulnerabilities have been growing steadily as well, impacting just 1% of applications in July–August and 6% in January–February (Figure 4). Similarly, serious XML external entity (XXE) vulnerabilities steadily impacted 1% of applications until November–December, when such vulnerabilities were found in 5% of applications. In January–February, XXE vulnerabilities were present in 6% of applications.

FIGURE 3

Percentage of applications containing at least one vulnerability and at least one serious vulnerability, four bimonthly periods.

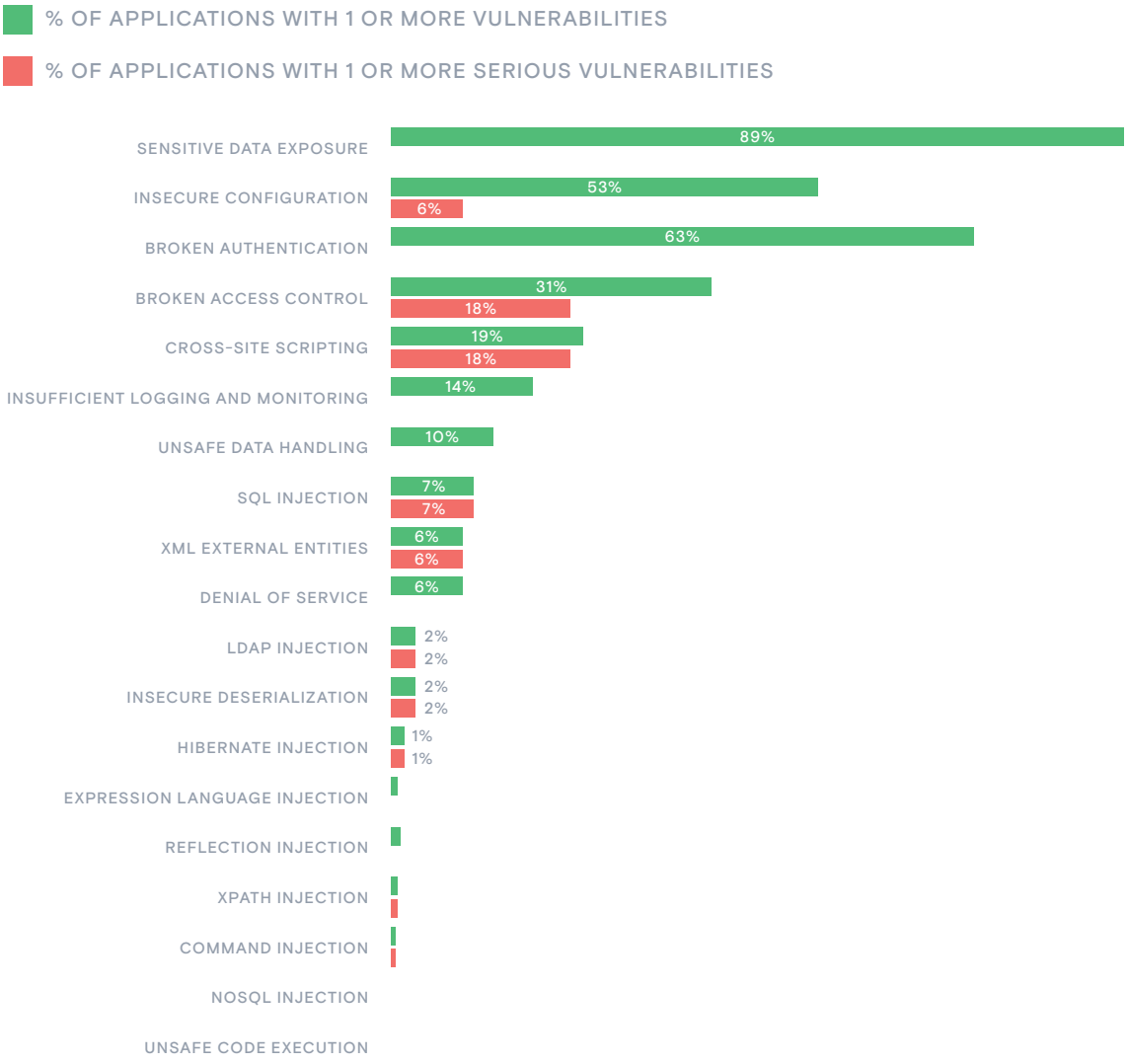


XXE attackers trick the XML parser into doing something unintended, such as exhausting memory, sending an attack to internal systems or to the local application, or in some cases, executing a system command. In a nutshell, an XXE vulnerability can turn a vulnerable application into a sort of internal, "behind the firewall" proxy for attackers to target internal systems. As the use of application programming interfaces (APIs) and microservices expands, we expect this trend to continue, and for similar increases to occur with other vulnerabilities related to parsing structured data from untrusted sources.

Another, less worrying trend is the steady growth in the percentage of applications with a sensitive data exposure vulnerability—up to 89% in January–February. Fortunately, none of these vulnerabilities is ranked as High or Critical, although 66% of them are rated Medium. This highlights the need for accurate and granular information to prioritize application security remediation.

FIGURE 4

Percentage of applications with vulnerabilities and serious vulnerabilities, by category, January–February 2021.



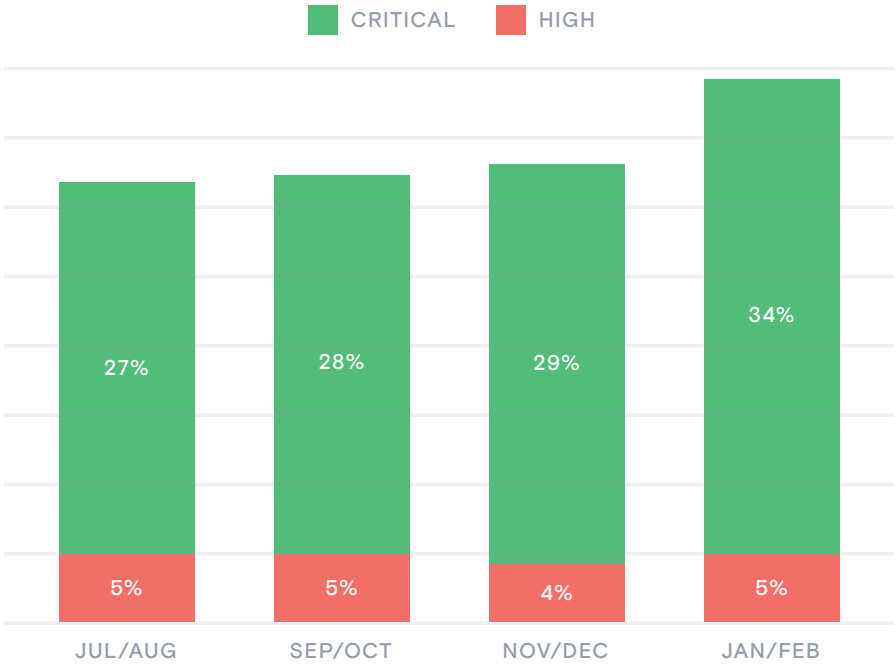
TREND: THE PERCENTAGE OF VULNERABILITIES THAT ARE SERIOUS CONTINUED TO RISE

The percentage of overall vulnerabilities rated as High or Critical continued to increase in January–February, sustaining a 10-month trend. In the current bimonthly period, 39% of vulnerabilities were rated as High or Critical, up from 33% in November–December (Figure 5). This represents an 18% jump in one bimonthly period.

Understanding the frequency of vulnerabilities can be useful in the context of a single application, as it can help developers understand whether a problem is systemic or a one-off. In many cases, systemic problems can be fixed in a single location. In other cases, a systemic problem might require changes to the software architecture to enable a centralized defense.

FIGURE 5

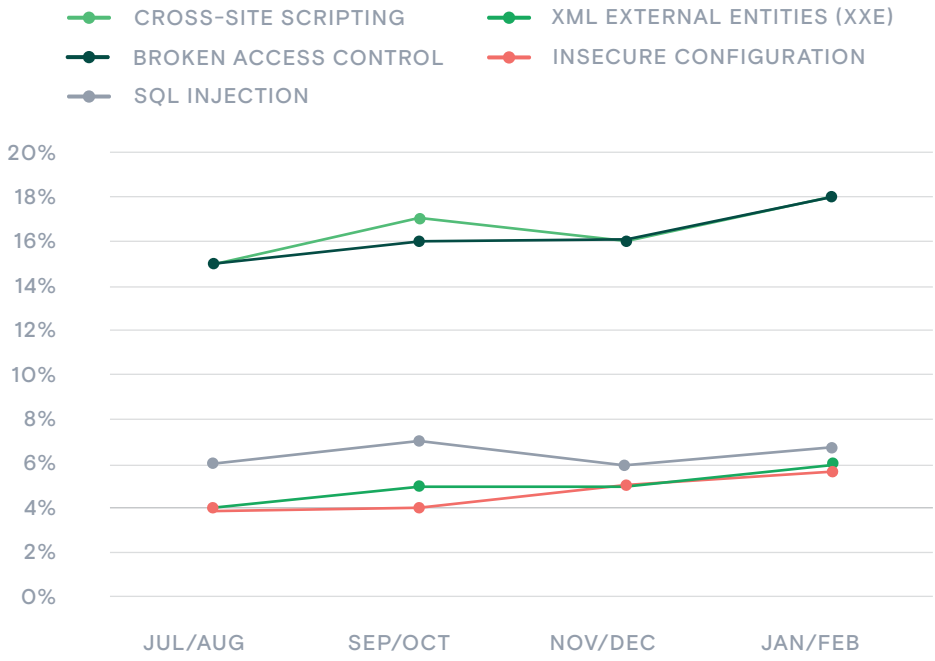
Percentage of vulnerabilities that are critical or high, four bimonthly periods.



This smaller increase in the prevalence of serious vulnerabilities is driven primarily by 2% increases in the percentage of applications with XSS and broken access control vulnerabilities, as well as a 1% increase in the percent of applications with XXE and insecure configuration vulnerabilities (Figure 6).

FIGURE 6

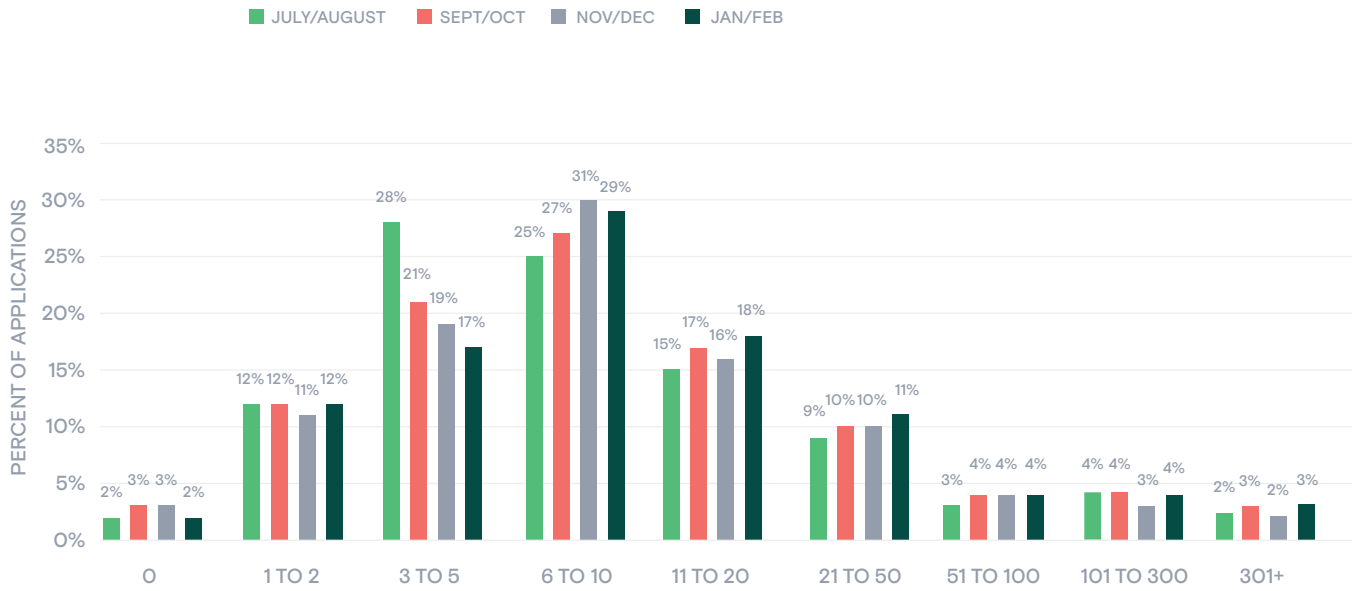
Percentage of applications with serious vulnerabilities (top 5 most prevalent).



Looking at vulnerability counts in applications, the percentage of applications with more than 50 vulnerabilities increased from 9% to 11%, but this change was a reversion to the mean after a decline in November–December (Figure 7). Among applications with at least one vulnerability, the average number of vulnerabilities rose from 56 to 61, but the average number of serious vulnerabilities per vulnerable application held steady at 58 (Figure 8).

FIGURE 7

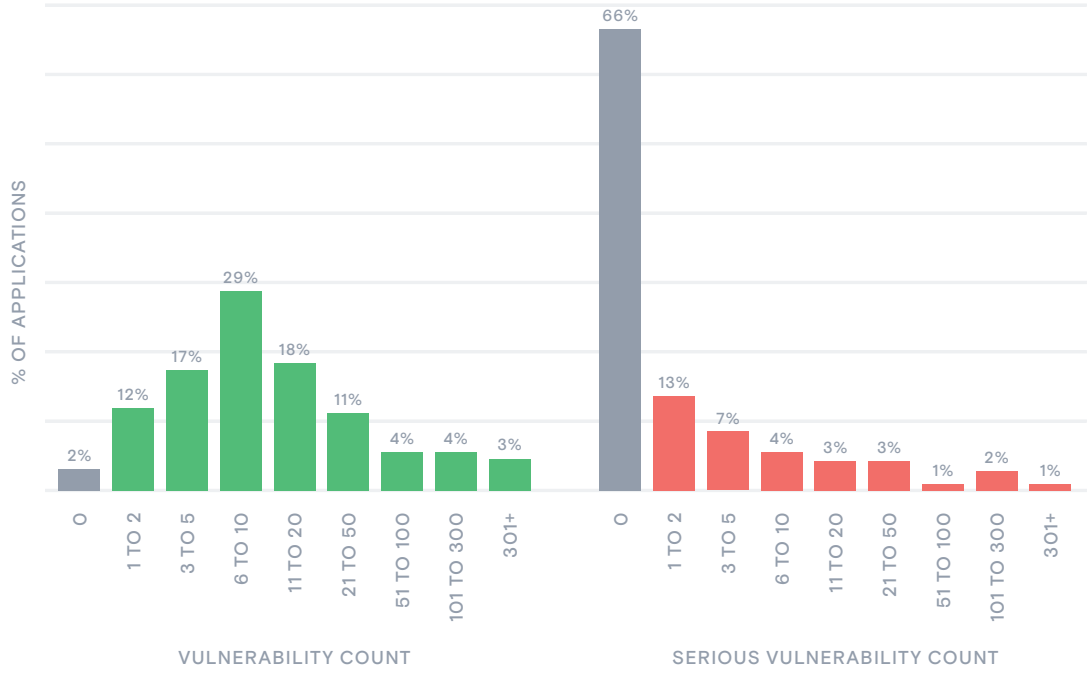
Percentage of applications with different numbers of vulnerabilities, four bimonthly periods.



Contrast SECURITY

FIGURE 8

Vulnerabilities and serious vulnerabilities per vulnerable application, four bimonthly periods.

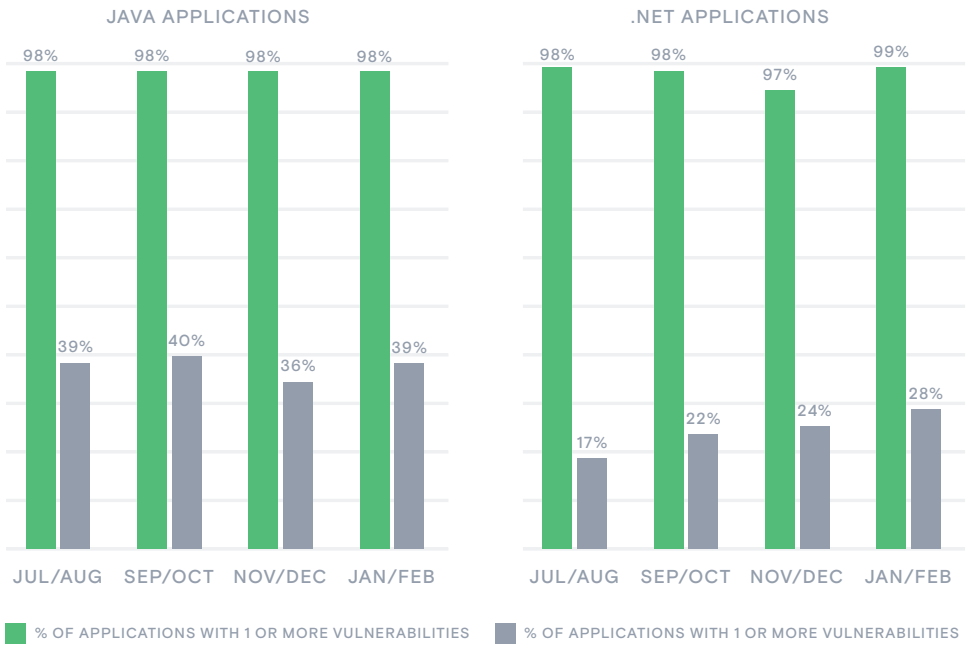


TREND: BOTH JAVA AND .NET SEE MORE APPLICATIONS WITH SERIOUS VULNERABILITIES

As noted in recent reports, the percentage of .NET applications that contain at least one serious vulnerability has been trending upward, reaching 28% in January–February (Figure 9). This is the highest percentage since an earlier spike in March–April of last year. Serious vulnerabilities impacted 39% of Java applications, up by three percentage points since the previous bimonthly period but a reversion to the mean. While .NET has long had the reputation for being less susceptible to vulnerabilities than Java, the threat is growing.

FIGURE 9

Overall vulnerabilities and serious vulnerabilities in Java and .NET applications, four bimonthly periods.

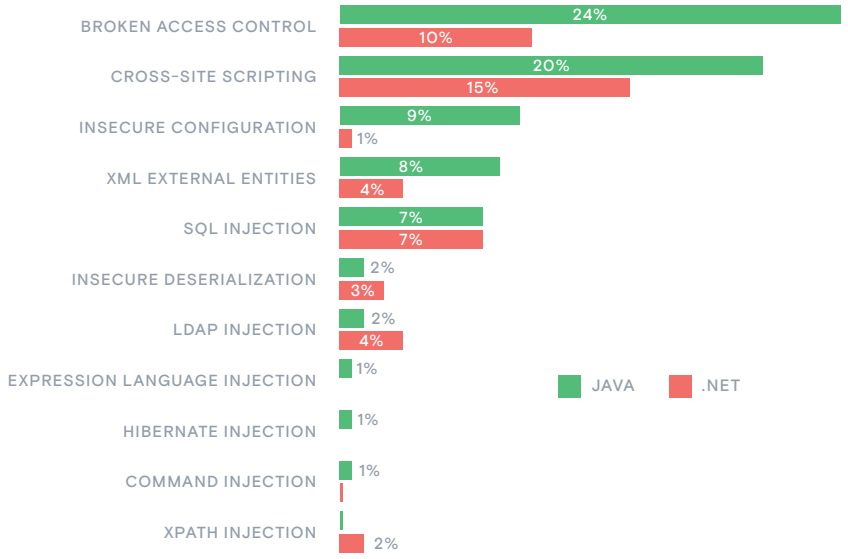


TREND: BOTH JAVA AND .NET SEE MORE APPLICATIONS WITH SERIOUS VULNERABILITIES

Looking at Java and .NET vulnerabilities by type, all of the top vulnerability types impacted a larger percentage of applications in January–February than in November–December. As a result, serious broken access control and XSS vulnerabilities impact a significant percentage of Java and .NET applications; 24% and 20% for Java applications and 15% and 10% for .NET applications (Figure 10). And serious XXE vulnerabilities increased by 40% in .NET applications, from 3% to 4%.

FIGURE 10

Percentage of Java and .NET applications impacted by serious vulnerabilities by category, January–February 2021.



05 Attack Trends

05 | Attack Trends

DATA FROM CONTRAST PROTECT DURING JANUARY AND FEBRUARY REVEALS THE FOLLOWING TRENDS REGARDING APPLICATION ATTACKS ON THE CUSTOM CODE IN APPLICATIONS:

TREND: AN EXCEEDINGLY HIGH PERCENTAGE OF ATTACKS WERE PROBES

As Contrast Labs has reported all along, the vast majority of attacks are probes and do not impact an actual vulnerability that exists in the targeted software. In January–February, that trend was even more pronounced, as less than 0.5% of attacks were viable—down from 2% in September–October and 1% in November–December (Figure 11). Of course, the purpose of a probe is to explore potential vulnerabilities that might be viable, so they are by no means harmless in the long run.

FIGURE 11

Percentage of attacks viable, four bimonthly periods.

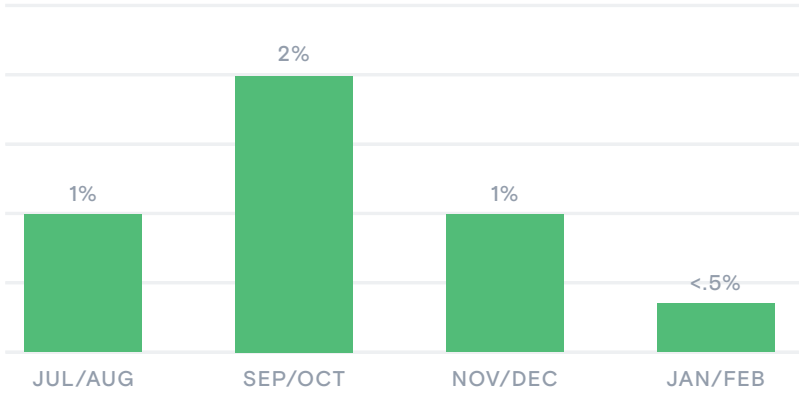
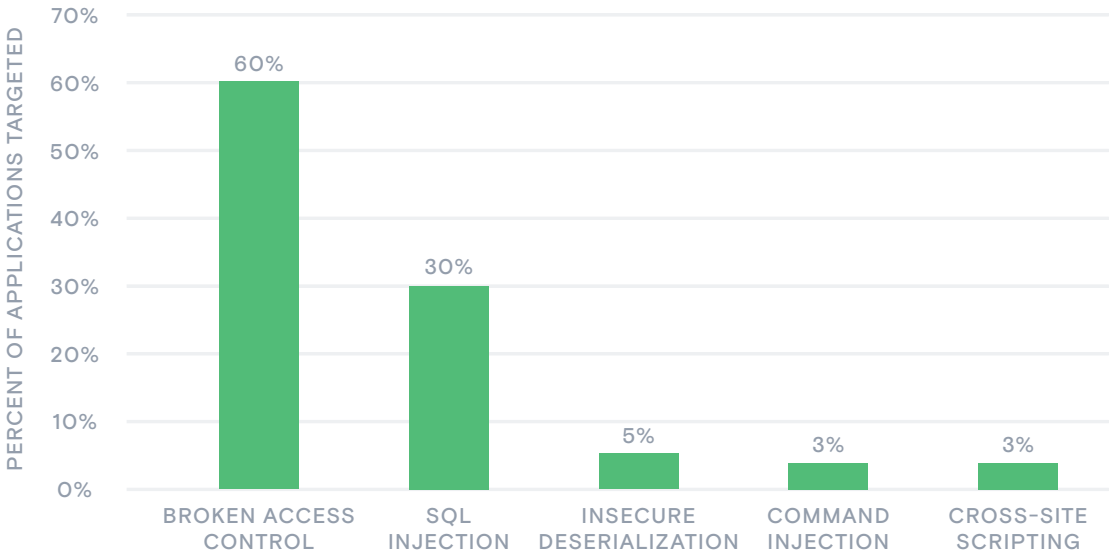


FIGURE 12

Percentage of overall attacks by category, January–February 2021.



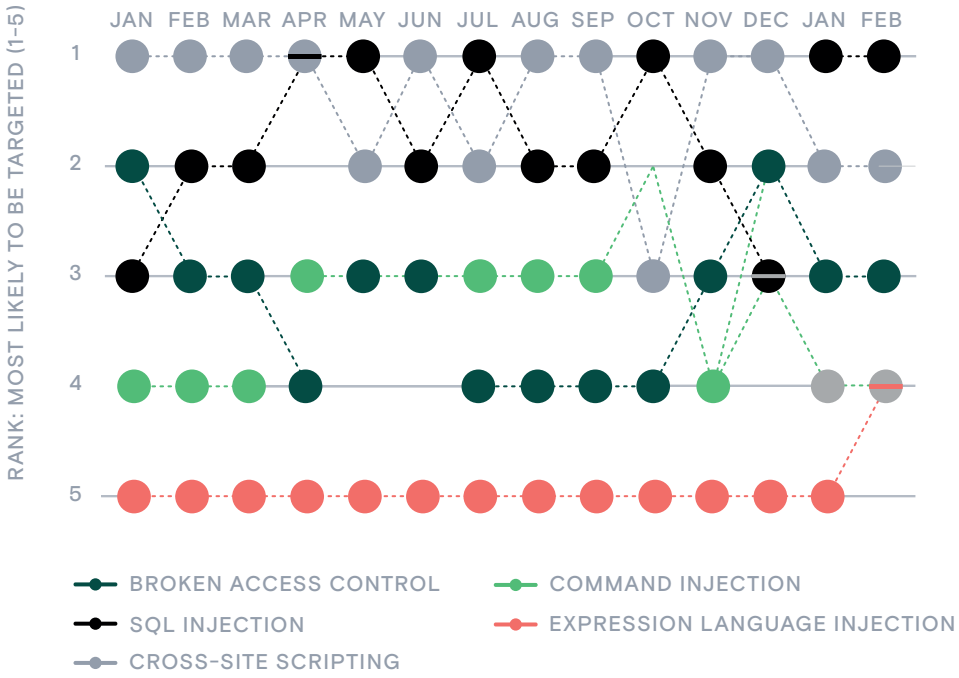
Contrast SECURITY

TREND: THE VAST MAJORITY OF ATTACKS WERE SQL INJECTION AND BROKEN ACCESS CONTROL

Among all attacks, two attack types represented 89.5% of attacks (i.e., those that reach their intended target)—SQL injection and broken access control (Figure 12). These two attack types have repeatedly alternated between the top two positions over the past year in terms of the highest percentage of attacks (Figure 13), and SQL injection retook the number one position for the first time since October. The remainder of the top five attack types remain consistent for the past year.

FIGURE 13

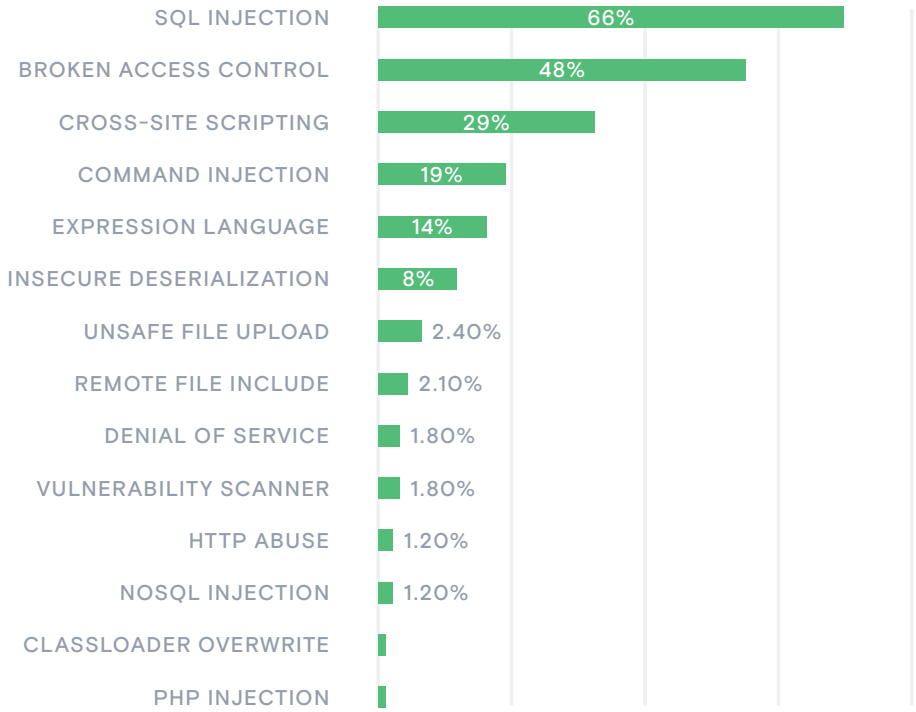
Rank of top 5 vulnerabilities most likely to be targeted, January 2020–February 2021.



Looking at which applications were impacted by different attack types, SQL injection and broken access control top this list also, with two-thirds of applications sustaining a SQL injection attack and nearly half on the receiving end of a broken access control attack (Figure 14).

FIGURE 14

Percentage of applications targeted by the top five attack categories, January–February 2021.



06 Conclusion

06 | Conclusion

Application security is taking center stage in 2021 after the devastating SolarWinds attack was revealed in December of last year. In the United States, the incoming administration quickly signaled that they intend to raise the profile of cybersecurity in the U.S. government.[11] More recently, reports of a forthcoming executive order[12] describe a possible application security scoring system that may be a part of the larger action.[13] The European Union, for its part, recently expressed solidarity with the U.S. in these efforts.[14]

In this context, accurate, actionable intelligence about application security is more important than ever for organizations trying to protect their vast software supply chain—including purchased software, third-party code, and the development infrastructure. Telemetry from custom code in actual applications in January–February revealed several disturbing trends, including an increased percentage of applications impacted by serious vulnerabilities for both Java and .NET applications. And while the fact that an even larger percentage of attacks were harmless probes can be comforting, these probes can provide intelligence for bad actors to aid with future attacks.

Contrast Labs hopes that this bimonthly report can help readers keep up with vulnerability and attack trends, and thereby intelligently prioritize their short-term application security efforts. Over time, the data can also help them refine their longer-term strategic plans. In both the short and the long term, it is increasingly clear that organizations should move beyond legacy approaches to application security.

Security instrumentation embeds continuous security testing and runtime protection within applications themselves. This provides continuous application security observability throughout the software development life cycle (SDLC). Actionable, real-time feedback enables developers to address problems as they occur. When using open-source software, organizations have visibility into which vulnerabilities pose risk and which are in code that is never used by the application. In production, instrumentation enables software to be self-protecting during runtime, stopping attacks before they cause damage. This comprehensive and continuous protection helps organizations to safely adopt today's rapid development timelines while providing protection against increasingly complex attacks.

[1] Charlie Osborne, "Everything you need to know about the Microsoft Exchange Server hack," ZDNet, April 19, 2021.

[2] Tom Burt, "New nation-state cyberattacks," Microsoft, March 2, 2021.

[3] Ax Sharma, "Sonatype Spots 275+ Malicious npm Packages Copying Recent Software Supply Chain Attacks that Hit 35 Organizations," Sonatype, February 12, 2021.

[4] Matt Austin, "Contrast Labs Reveals Dependency Confusion Vulnerability in Microsoft Teams," Contrast Security, March 4, 2021.

[5] Lawrence Abrams, "Malicious npm packages target Amazon, Slack with new dependency attacks," BleepingComputer, March 2, 2021; Henri Terho, "Dependency Confusion attack 16.2.2021," Qentinel, February 18, 2021.

[6] Jessica Haworth, "Zero-day vulnerability in SonicWall products actively exploited in the wild," The Daily Swig, February 4, 2021.

[7] Tara Seals, "Amazon Kindle RCE Attack Starts with an Email," Threatpost, January 22, 2021.

[8] John Leyden, "Multiple new flaws uncovered in SolarWinds software just weeks after high-profile supply chain attack," The Daily Swig, February 3, 2021.

[9] "RiskScore Index Report," Contrast Security, February 3, 2021.

[10] "2021 State of Open-Source Security Report," Contrast Security, April 8, 2021.

[11] John Leyden, "Incoming Biden administration looks to shake up US cybersecurity policy," The Daily Swig, January 19, 2021.

[12] Sean Lyngaas, "After SolarWinds breach, White House preps executive order on software security," CyberScoop, March 5, 2021.

[13] Tim Starks, "Biden administration mulls software security grades after SolarWinds," CyberScoop, March 12, 2021.

[14] "E.U.'s Borrell voices solidarity with US in SolarWinds hack," The Associated Press, April 15, 2021.

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