# State of Attacks2025

Annual report

Learn about Continuous Hacking's year-long findings and how they can inspire you to improve your cybersecurity posture.

SECTION 01

## Introduction

At **Fluid Attacks**, as an application security (AppSec) company, we are dedicated to helping our clients identify, prioritize, and remediate security vulnerabilities in their software products by integrating various automated tools, artificial intelligence models, and a highly certified team of pentesters.

**In 2024**, we assessed and contributed to the security of our clients' systems through our comprehensive **Continuous Hacking** solution during the entire software development lifecycle (SDLC). When we refer to a system, it may include all three, two, or just one of the following targets of evaluation: **application source code**, **running application**, and **infrastructure**.*

The **State of Attacks 2025** report, like those from previous years, can help you benchmark and improve your company's cybersecurity posture. Many of the conclusions we drew after reviewing a full year of data from security testing and management can serve you as a guide for setting more effective goals, focusing on secure development practices and rapid vulnerability remediation to protect your systems, data, operations, and users.

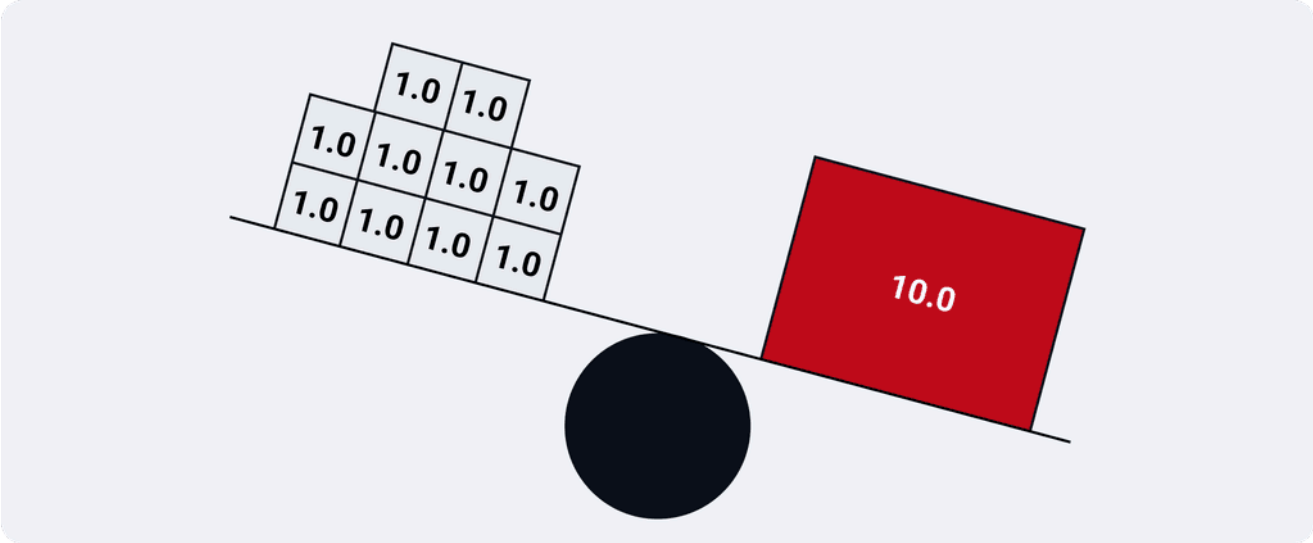
**Data collection period: Jan 1 - Dec 31, 2024**
*Hereinafter, "source code, "application," and "infrastructure," respectively.

### Focus on risk exposure rather than the number of vulnerabilities

Before delving into the findings for 2024 as a whole, it is important to note that at Fluid Attacks, we recognize that the fact that a system has **few vulnerabilities is not synonymous with a high level of security**. The key is to keep the **risk exposure** to a minimum. In other words, for example, having ten vulnerabilities with a CVSS score of **1.0** in a system does not represent the same degree of risk exposure as having one vulnerability with a score of **10.0**. Based on this reasoning, we developed **the CVSSF metric**, a modification of the CVSS score that allows organizations to prioritize their vulnerability remediation efforts more effectively.

**The CVSSF overcomes many of the shortcomings of the CVSS**, such as aggregation and comparison, providing clearer visibility of the magnitude of risk exposure. Thus, following the example in the previous paragraph and the CVSSF equation,* as we can see in the illustration, those ten vulnerabilities on the left side of the balance merely reach a CVSSF of **0.2**. In contrast, the vulnerability on the right has a huge value of **4,096.0**, a comparison of values closer to the reality of risks.

*CVSSF = 4^(CVSS-4)




SECTION 02

## Executive summary

Check out the most impactful results

[1]

The number of systems we assessed for security using Continuous Hacking in 2024 grew by **27.6%** in comparison to 2023.

[2]

Although we reported **59.3%** more vulnerabilities than the previous year, total identified risk exposure (CVSSF units) decreased by **3.8%**.

[3]

This year, on average, organizations took **18.5%** less time to remediate their security vulnerabilities. Moreover, the mean time to remediate critical-severity issues decreased by a considerable **65%**.

[4]

Vulnerability remediation in systems that broke the build took, on average, **50%** less time compared to those that did not.
[5]

The remediation rate for systems that broke the build was **62.4%**, while for those that did not, it was 31.5%.

[6]

Our pentesters, compared to our automated tools, reported **71%** of the total risk exposure.

[7]

**Almost 99%** of critical-severity vulnerabilities were detected by our pentesters (our tool had already found the rest).

[8]

The most persistent security weakness among the assessed systems was "**Unverifiable files**."

[9]

The weakness that represented the highest total risk exposure during the year was "**Improper authorization control for web services**."

[10]

High- and critical-severity vulnerabilities showed the best cumulative remediation rates at the end of the year, with **57.4%** and **73.2%**, respectively.
SECTION 03

## Prominent changes

Spot the key differences compared to the previous report

### Assessed systems

The number of systems we evaluated with **Continuous Hacking** increased by **27.6%** compared to the previous year.* In addition, 57.6% of the systems under assessment with our solution in 2023 continued to be evaluated in 2024, a year in which nearly 55% of the systems were new.

## 27.6%

/ Continuous Hacking
*We emphasize that this is a comparison limited to the Continuous Hacking solution. In 2023, there were still a few systems being tested with our One-Shot Hacking solution, no longer offered.

### Risk exposure

In 2024, from Continuous Hacking, we reported **a total risk exposure 3.8% lower** than in 2023. It dropped from about 32.5 million to 31.3 million units (following our CVSSF metric). Accordingly, the mean and median risk exposure per system decreased by 24.6% and 33.2%, respectively.

## 3.8%

## 24.6%

/ Mean

## 33.2%

/ Median

### High and critical severity vulnerabilities

**62.3%** of all systems under assessment showed **at least one high- or critical-severity vulnerability**, representing a reduction with respect to the previous year, when that figure stood at 66.6%.

## 66.6%

## 62.3%

### Rating

### CVSSv4.0 score

Critical

9.0 - 10.0

High

7.0 - 8.9
Medium

4.0 - 6.9

Low

0.1 - 3.9

None

0.0

### Manual detection methods

We constantly improve our tools in terms of their scope and vulnerability detection capabilities, yet **our team of pentesters continues to achieve much higher results** in terms of risk exposure and critical-severity vulnerabilities identified. The percentages achieved with their manual testing varied little in the compared periods.

## 71.4%

## 71.1%

/ Risk exposure

## 97.1%

## 98.9%

/ Critical vulnerabilities

### Vulnerability remediation

The mean time to remediate (MTTR) vulnerabilities was **about 55 days**. This is a **reduction of almost 19%** compared with the 68 days of the previous year. Furthermore, it should be noted that the MTTR for critical severity vulnerabilities was reduced by a significant **65%**.

## 18.5%

/ MTTR

## 65.0%

/ MTTR for critical vulnerabilities

In line with previous years' reports, remediation times for security issues in systems where companies chose to **break the build** were shorter than in those where companies decided not to do so. However, the median time to remediate vulnerabilities for build breakers changed from **19** to **28 days** with respect to the prior report.

- **Time to remediate:** Time elapsed between the reporting of a vulnerability and its remediation.
- **Break the build:** Security control for CI/CD pipelines in which our CI Gate interrupts software deployment whenever there are still unaccepted vulnerabilities in the product.

SECTION 04

# General findings

Explore the year’s vulnerability and risk exposure landscape

□

## 872,612

Reported vulnerabilities

## 824

Mean number of vulnerabilities by system

## 31,295,535

Reported risk exposure (CVSSF units)

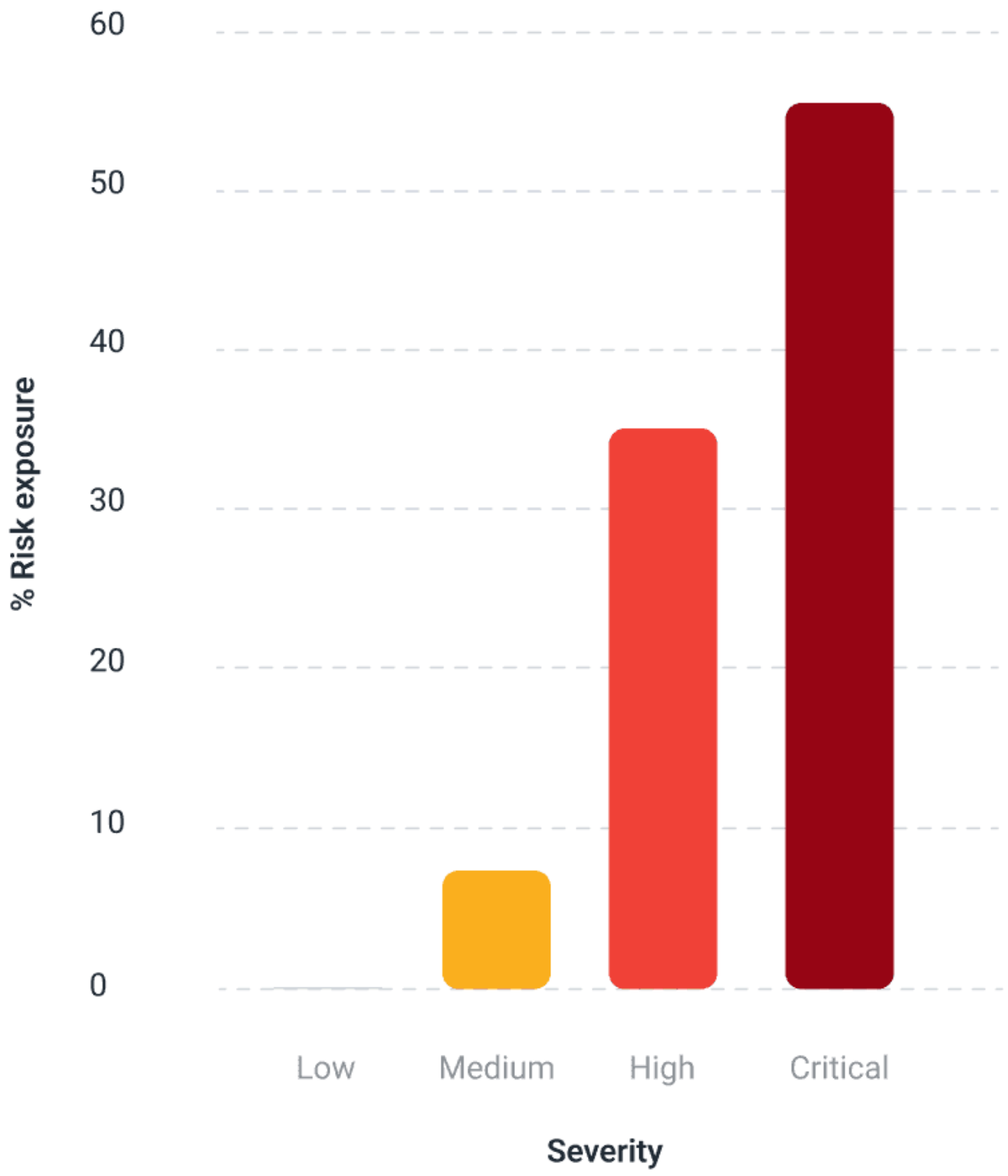
## 29,552

Mean risk exposure by system

### Risk exposure by severity

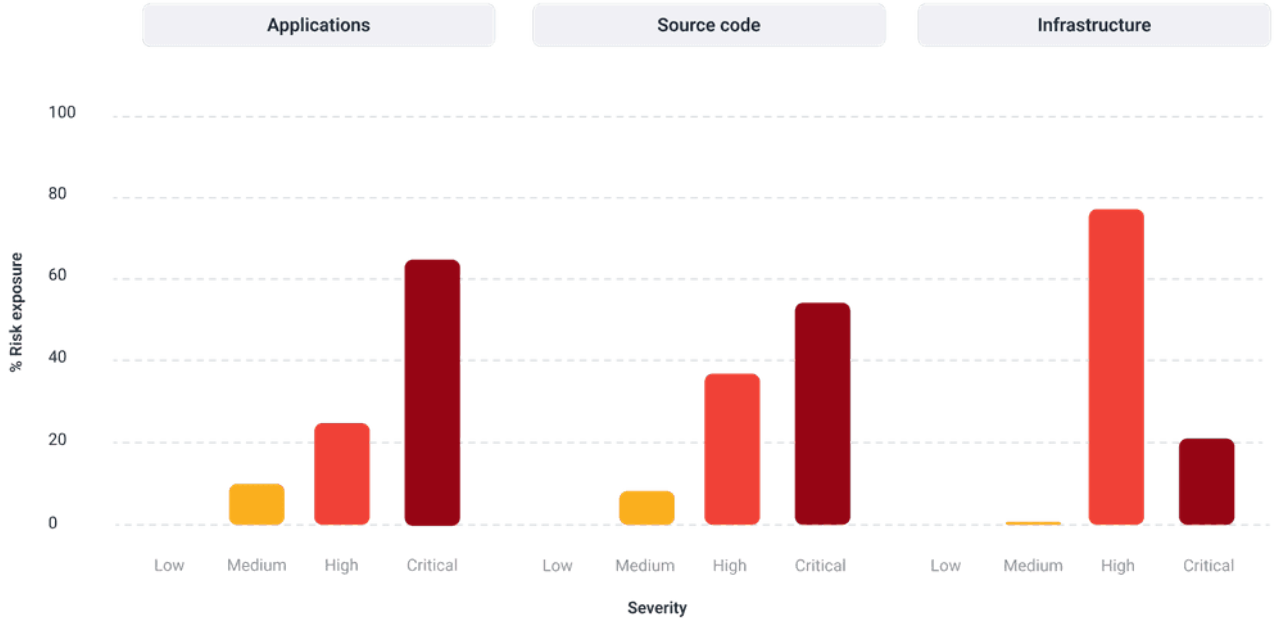
Nearly all of the risk exposure in the systems evaluated, i.e., **91.6%**, was due to high- and critical-severity vulnerabilities. This means that a small fraction, just **5.1%**, of the security issues identified were responsible for a risk exposure **almost 11 times** the value summed up by all medium- and low-severity vulnerabilities.

| Severity | Total vulnerabilities | Total risk exposure |
| --- | --- | --- |
| Critical | 10,802 | 17,456,578.79 |
| High | 34,009 | 11,197,833.43 |
| Medium | 126,110 | 2,620,324.37 |
| Low | 701,691 | 20,798.08 |




**Vulnerabilities and risk exposure by severity**

For each target of evaluation


In applications and source code, the same pattern of decreasing number of vulnerabilities as their severity range increased was maintained. In the case of infrastructures, high-severity vulnerabilities broke this pattern. However, it must be taken into account that very few organizations requested an infrastructure assessment, resulting in a limited number of vulnerabilities detected for this type of target.

Now, focusing on those two most frequent targets, we can say that low- and medium-severity vulnerabilities accounted for more than **ninety percent of all security issues** detected (i.e., **96.5%** for applications and **94.7%** for source code). Nevertheless, it was the high- and critical-severity vulnerabilities that together exceeded ninety percent for the **total risk exposure** across all targets, including infrastructure.

| Target of evaluation | Total vulnerabilities | Total risk exposure |
| --- | --- | --- |
| Source code | 799,072 | 28,202,146.76 |
| Application | 73,475 | 3,068,326.34 |
| Infrastructure | 65 | 25,061.57 |

**Risk exposure by detection method**

## 28.9%

/ Automatic (SAST, SCA, DAST, CSPM*)

## 71.1%

/ Manual (PTaaS, SCR, RE**)

## 22,246,515.93

/ Manual

## 9,049,018.73

/ Automatic

***SAST:** static application security testing

**SCA:** software composition analysis

**DAST:** dynamic application security testing

**CSPM:** cloud security posture management

****PTaaS:** penetration testing as a service

**SCR:** secure code review

**RE:** reverse engineering

If we look at all the vulnerabilities detected in 2024 and their associated risk exposure, those discovered by our automated tools represented, on average, **12.7 CVSSF units**. In contrast, those found by our pentesters reached an average of **eleven times** that value: **139.7 CVSSF units**.

As mentioned in previous State of Attacks reports, security testing by our pentesters continues to reveal greater amounts of risk exposure than our automated tools.

Moreover, the figures shown here could have been even more favorable for our experts if all systems had been evaluated within our **Advanced plan**, which includes **automated and manual security testing**. However, some of them were only subscribed to our Essential plan, which includes only automated testing.

No matter how many tools your company employs or how adept you are at the current AI trend, exhaustive cybersecurity posture assessments still depend on the inclusion of the human factor. **A comprehensive AppSec solution must leverage the advantages of security experts, AI, and scanners**.

As further support for the last statement, we recommend reading our research report "Boosting AST accuracy through pentesting."

### Vulnerabilities by detection method

**More than eighty percent** of the total vulnerabilities were identified by our automated tools. Furthermore, if we consider the **44,811** high- and critical-severity vulnerabilities found during the year, we can see that these tools detected **55.2%** of them.

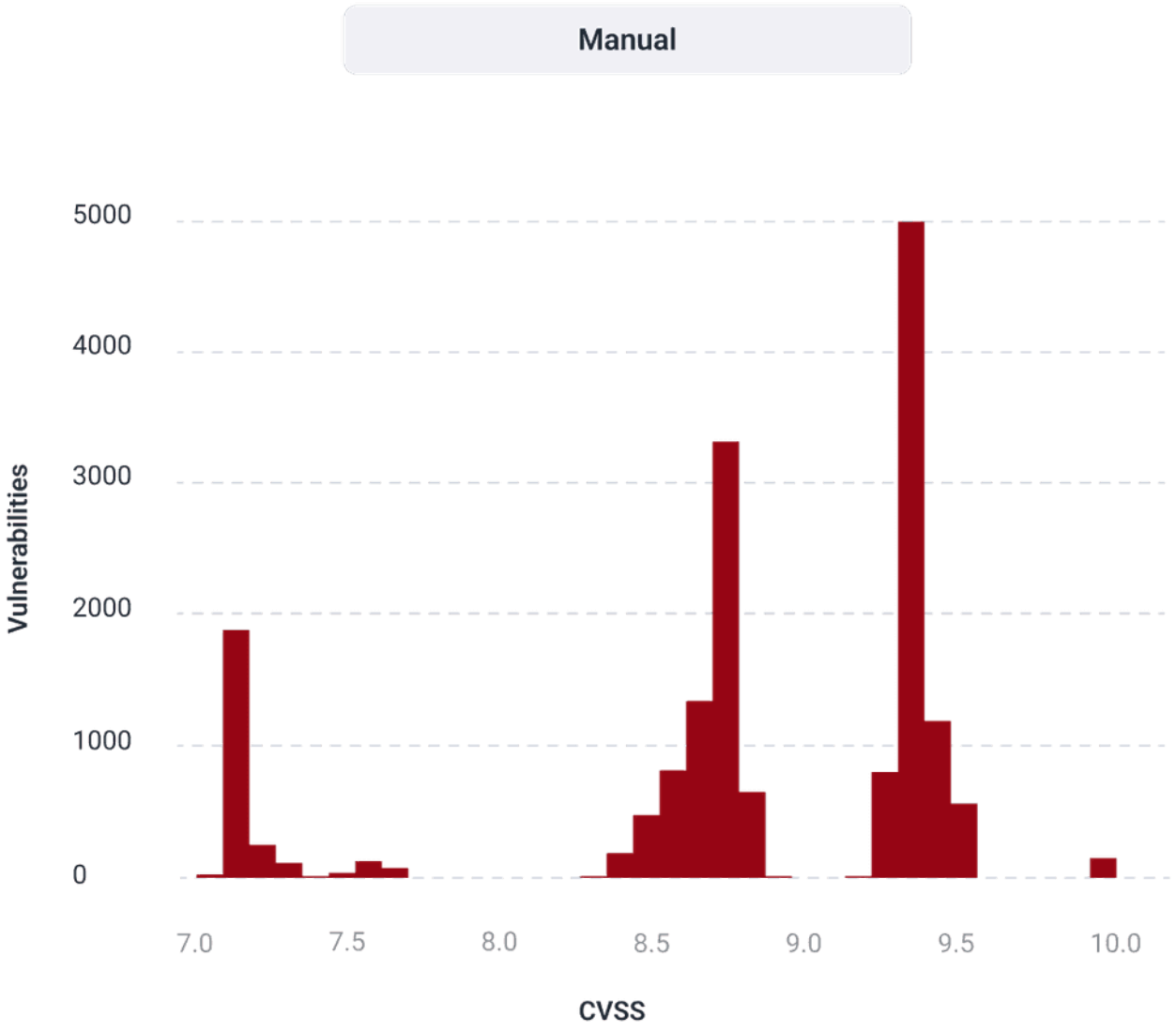
## 81.8%

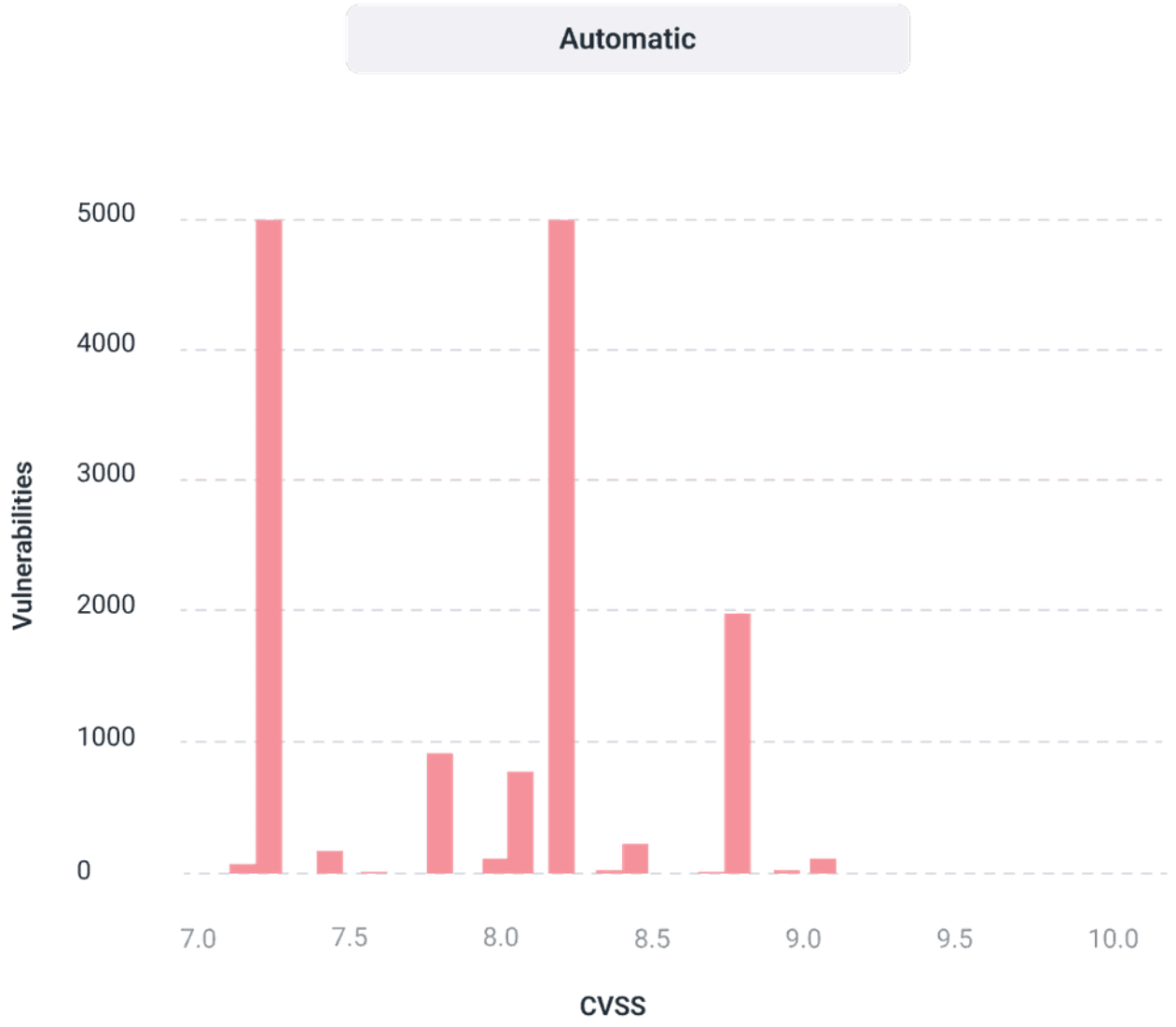
/ Automatic

## 18.2%

/ Manual

However, **if we take only critical-severity vulnerabilities**, a staggering **98.9% were identified through manual analysis**. This highlights, as seen in previous years, the greater effectiveness of PTaaS and other types of manual testing in uncovering the most serious security flaws compared to vulnerability scanning.






SECTION 05

## Top weaknesses

Get to know the key vulnerabilities by risk and persistence

### Top 10 weaknesses

By risk exposure

Starting in the second half of 2024, we decided to discontinue the weakness categories "011. Use of software with known vulnerabilities," "393. Use of software with known vulnerabilities in development," and "435. Use of software with known vulnerabilities in environments."* These categories associated with third-party software dependencies or components were very general, meaning they did not specify the types of vulnerabilities present within the

packages used. This, precisely, along with the enormous use we all make of third-party open-source components in our products, was what caused these categories to top the lists in our previous reports.
***The discontinuation was gradual and completed in early 2025. This is why you can find remaining cases from those categories in this report.**

Thus, on this occasion, the weakness that topped the ranking was "**Improper authorization control for web services**." This persistent issue, which once exploited, could allow attackers to obtain confidential information, accounted for over **27% of the total risk exposure** reported in 2024. Moreover, the weaknesses within this top 10 list contributed to **77.2% of the overall risk exposure**.

Weakness

Systems

Persistence

Exposure

MEx

039. Improper authorization control for web services

263

10,356

8,490,025.9

819.8

006. Authentication mechanism absence or evasion

161

7,463

7,690,775.4

1,030.5

096. Insecure deserialization

173

13,262

1,947,603.2

146.9

100. Server-side request forgery (SSRF)

304

7,053

1,724,486.6

244.5

359. Sensitive information in source code - Credentials

331

13,415

893,774.0

66.6

011. Use of software with known vulnerabilities

390

19,390

871,626.9

45.0

390. Prototype pollution

234

11,236

800,728.7

71.3

076. Insecure session management

76

721

770,025.0

1068.0
211. Asymmetric denial of service - ReDoS

354

21,587

555,517.4

25.7

422. Server side template injection

178

2,845

419,534.5

147.5

- **Weakness:** The category, while the vulnerability is the particular case with a specific location that belongs to the category.
- **Persistence:** Number of vulnerabilities identified belonging to the category.
- **MEx:** Mean risk exposure.

**Top 10 weaknesses**

---

By the number of systems

The weakness we detected **in more than half of the systems** evaluated is related to the inability to verify files in repositories because their content is not compatible with their extension: "**Unverifiable files**." This issue, along with the others listed in the table, constituted **35.6% of the total vulnerabilities detected**. Still, their mean and median temporary CVSS scores did not exceed the medium severity range.

Looking at other data in the table below, we can highlight that the weakness "**Sensitive information in source code**" appeared in **around 40%** of the systems evaluated, but its MTS and MdTS were quite low, which explains why it did not appear in the table above. However, when we focus on a similar but more specific and risky weakness, such as "**Sensitive information in source code - Credentials**," we notice that it ranked **fifth** among the security issues that represented the highest risk exposure in 2024.

Weakness

Systems

Persistence

MTS

MdTS

117. Unverifiable files

540

183,708

0.6

0.6

431. Supply chain attack - Lock files

473

18,041

0.6

0.6

052. Insecure encryption algorithm

430

6,270

2.0

0.6

009. Sensitive information in source code

425

10,202

2.2

1.3

380. Supply chain attack - Docker

394

10,788

0.6

0.6

011. Use of software with known vulnerabilities

390

19,390

4.4

4.6

097. Reverse tabnabbing

383

22,550

1.1

1.1

266. Excessive privileges - Docker

371

7,395

1.3

1.1

211. Asymmetric denial of service - ReDoS

354

21,587

5.4

6.6
002. Asymmetric denial of service

351

10,655

5.7

6.6

- **MTS:** Mean CVSS temporal score.
- **MdTS:** Median CVSS temporal score.

**Top 5 weaknesses**

Target of evaluation: source code

By risk exposure

**This top 5 is exactly the same** as the one found in the overall top 10 table for risk exposure. **Almost all** vulnerabilities belonging to these five categories were located in the evaluated source code. Although their combined persistence accounted for just **over 6%** of the total vulnerabilities identified in this type of target, their combined risk exposure accounted for **almost 70%** of the total detected in source code.

"**Authentication mechanism absence or evasion**" was the least reported among all weaknesses listed here. However, it ranked second among all weaknesses detected in the year regarding risk exposure, constituting **22.6% of the total**.

Weakness

Systems

Persistence

Exposure

MEx

039. Improper authorization control for web services*

238

9,680

8,009,170.8

827.4
006. Authentication mechanism absence or evasion

127

6,730

7,078,979.2

1,051.9

096. Insecure deserialization

173

13,262

1,947,603.2

146.9

100. Server-side request forgery (SSRF)

301

7,017

1,713,775.2

244.2

359. Sensitive information in source code - Credentials

329

13,403

893,760.1

66.7
*__Recommendation:__ Validate through session cookies or tokens that users trying to access certain information are authenticated.

**Top 5 weaknesses**

Target of evaluation: application

By risk exposure

Although in inverted order, the two weaknesses that led the following top 5 were the same as those that led the top 10 for risk exposure. While all vulnerabilities found in these categories accounted for only **about 3.0%** of the total identified in the applications, their cumulative risk exposure constituted **54.9%** of the total in this target of evaluation.

In third place, we have the weakness "**Account takeover**," which, with **the highest MEx** on this list, represents the risk of an attacker exploiting one or more vulnerabilities in the application to take control of a user account and perform actions on their behalf.

Weakness

Systems

Persistence

Exposure

MEx

006. Authentication mechanism absence or evasion*

81

732

611,790.1

835.8

039. Improper authorization control for web services

77

674

480,686.1

713.2

417. Account takeover

57

214

266,332.3

1,244.5

005. Privilege escalation

47

281

193,690.4

689.3

146. SQL injection

35

291

132,905.7

456.7
*__Recommendation:__ Every functional resource critical to the organization must have a robust authentication process, and it is necessary to ensure that every user attempting to access them has an initialized session.
SECTION 06

## Vulnerability remediation

Discover remediation times and rates based on various factors

**All vulnerabilities**

## 41.0%

/ Remediated

## 1.3%

/ In progress

## 7.2%

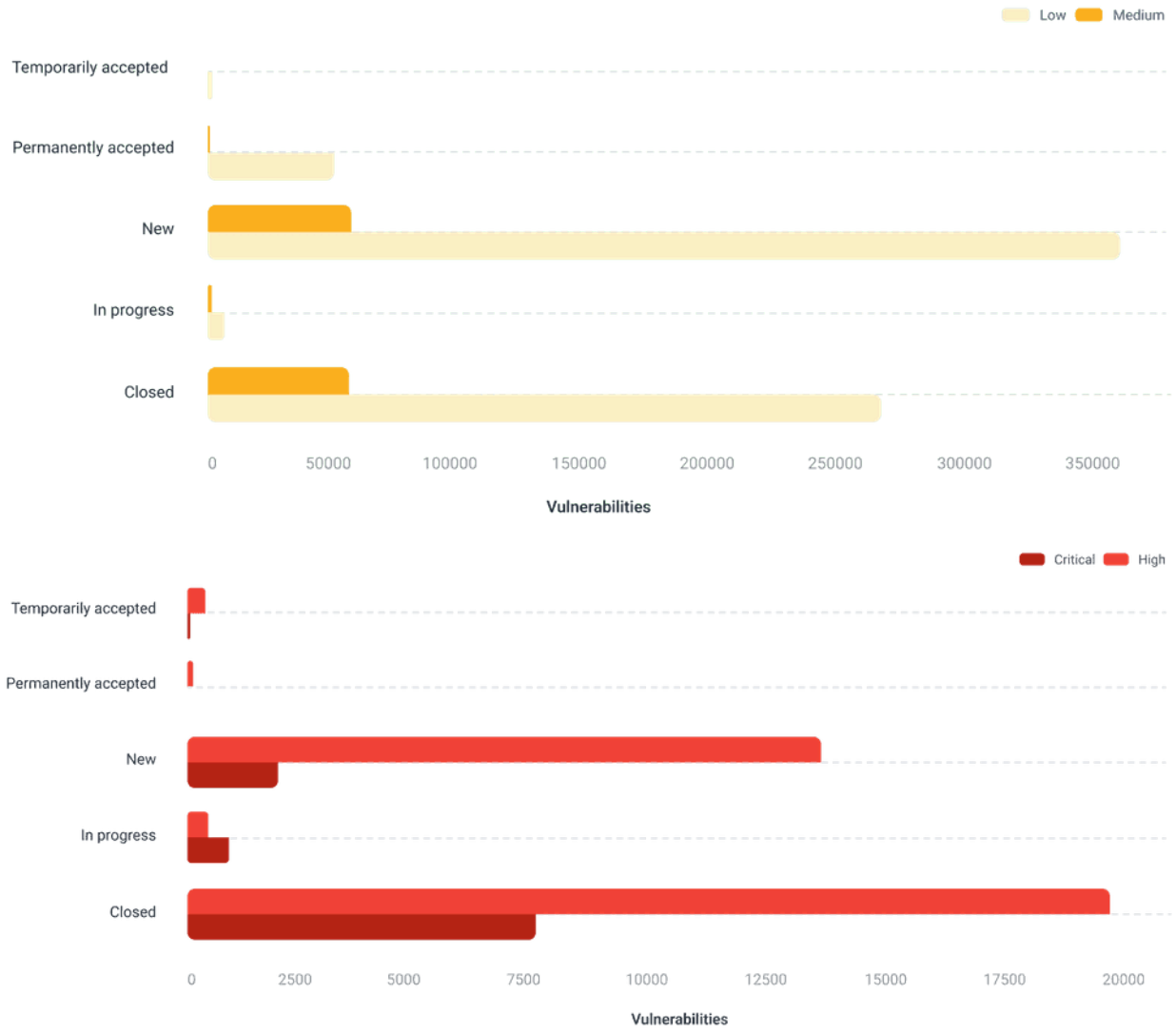
/ Accepted

## 50.5%

/ New

**Less than half** of the identified vulnerabilities were remediated. Systems that **broke the build** had a remediation rate of **62.4%** by the end of the year, significantly higher than those that did not, which had a rate of **31.5%**.

Examining the severity ranges across all systems, the cumulative remediation rates for low-, medium-, **high-**, and **critical-severity** vulnerabilities were 38.3%, 49.1%, **57.4%**, and **73.2%**, respectively. It is noteworthy that only **0.34%** of high-severity vulnerabilities and **0.05%** of critical-severity vulnerabilities were permanently accepted, although ideally these values should be zero.




- **New:** The organization has not yet defined treatment for the vulnerability.
- **In progress:** The organization already has plans to remediate the vulnerability.
- **Closed:** The organization has already remediated the vulnerability.

- **Temporarily accepted:** The organization has decided not to remediate the vulnerability for the moment.
- **Permanently accepted:** The organization has decided not to remediate the vulnerability.

**Time to remediate**

Median days for vulnerability remediation

## 28

/ Breaking the build

## 56

/ Not breaking the build

When comparing the medians, we found that companies took **50% less time** to remediate vulnerabilities in systems where they **broke the build** than in those where they did not.

By differentiating remediation times according to severity ranges, it was the medium range that was the exception or broke the expected pattern, which states that **the greater the severity, the fewer days should be spent in remediation**. If we compare the MTTRs and MdTTRs of the extreme ranges, we see an appropriate performance: Teams spent **27.1%** and **22.2% less time**, respectively, remediating critical-severity vulnerabilities than low-severity ones.

In fact, in **63.3%** of all systems where critical vulnerabilities were remediated, **MTTRs were lower than the overall MTTR for this range (43 days)**. However, **12.2%** had MTTRs between 80 and 143 days, and **2.0%** had MTTRs greater than 239 days, which warrants reflection, given the risk posed by these security issues. It should also be noted that **more than half of all critical-severity vulnerabilities remediated were resolved in less than 34 days.**

Severity

MTTR

MdTTR

Remediated vulnerabilities

Low

59

36

268,710
Medium

43

24

61,886

High

49

51

19,506

Critical

43

28

7,907

- **MTTR:** Mean time to remediate.
- **MdTTR:** Median time to remediate.

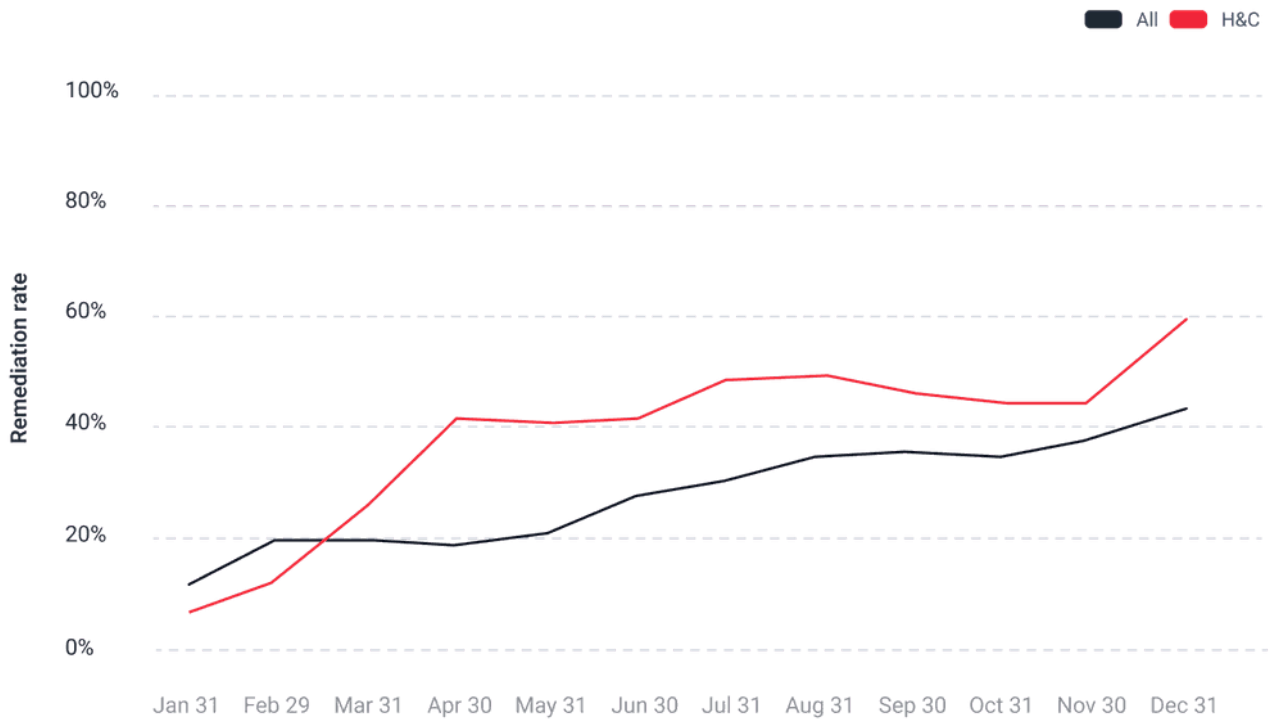
### Remediation rate over time

All vs high- and critical-severity vulnerabilities

Usually, more vulnerabilities were discovered than fixed each month.* However, the cumulative remediation rate for all identified vulnerabilities generally increased over time, going from an initial 13.5% to 41.0% at the end of the year (the average remediation rate was **27.6%**).

Meanwhile, the accumulated remediation rate for high- and critical-severity vulnerabilities consistently outpaced the overall rate, and, contrary to the previous year, showed an upward trend. In fact, its minimum value was 8.8% at the end of January and its maximum value was 61.2% at the end of December. Thus, its average remediation rate was **40.4%**, which is closer to that obtained for high-severity vulnerabilities than for critical-severity ones (you can compare the following two graphs to appreciate this).

*For this and the next analysis, we took the accumulated number of vulnerabilities reported and remediated throughout the year by the end of each month. It should be noted that for the end of January, we recorded as remediated vulnerabilities only those that were identified and closed during that month. However, for the following months, we recorded as remediated those closed during the given month, regardless of the month they were detected in 2024.

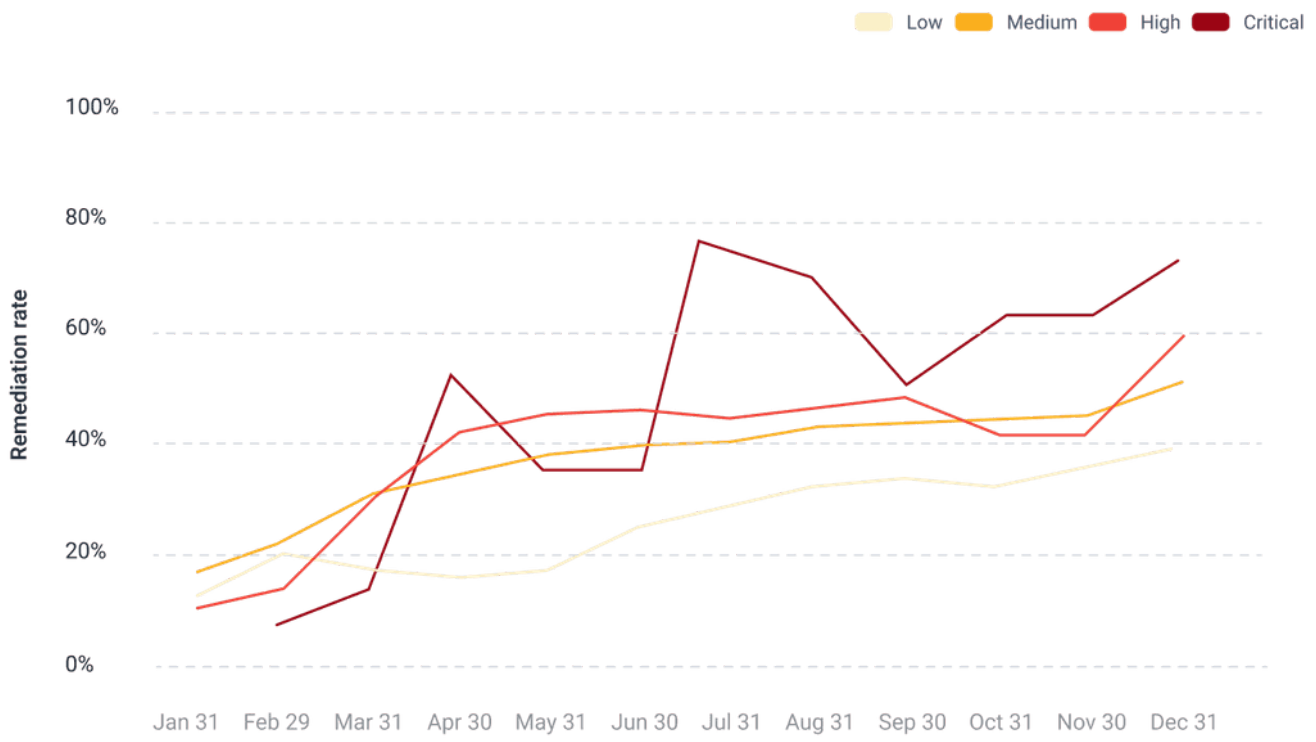



**Remediation rate over time**

By severity

For **about half the year**, the accumulated remediation rates followed a usually **expected pattern**, being higher as the severity range increased. The sharpest changes among the four severity ranges occurred in the remediation rates for critical-severity vulnerabilities. The lowest average remediation rate was for low-severity vulnerabilities, at **25.5%**, and the highest was for critical-severity vulnerabilities, at **45.2%**.

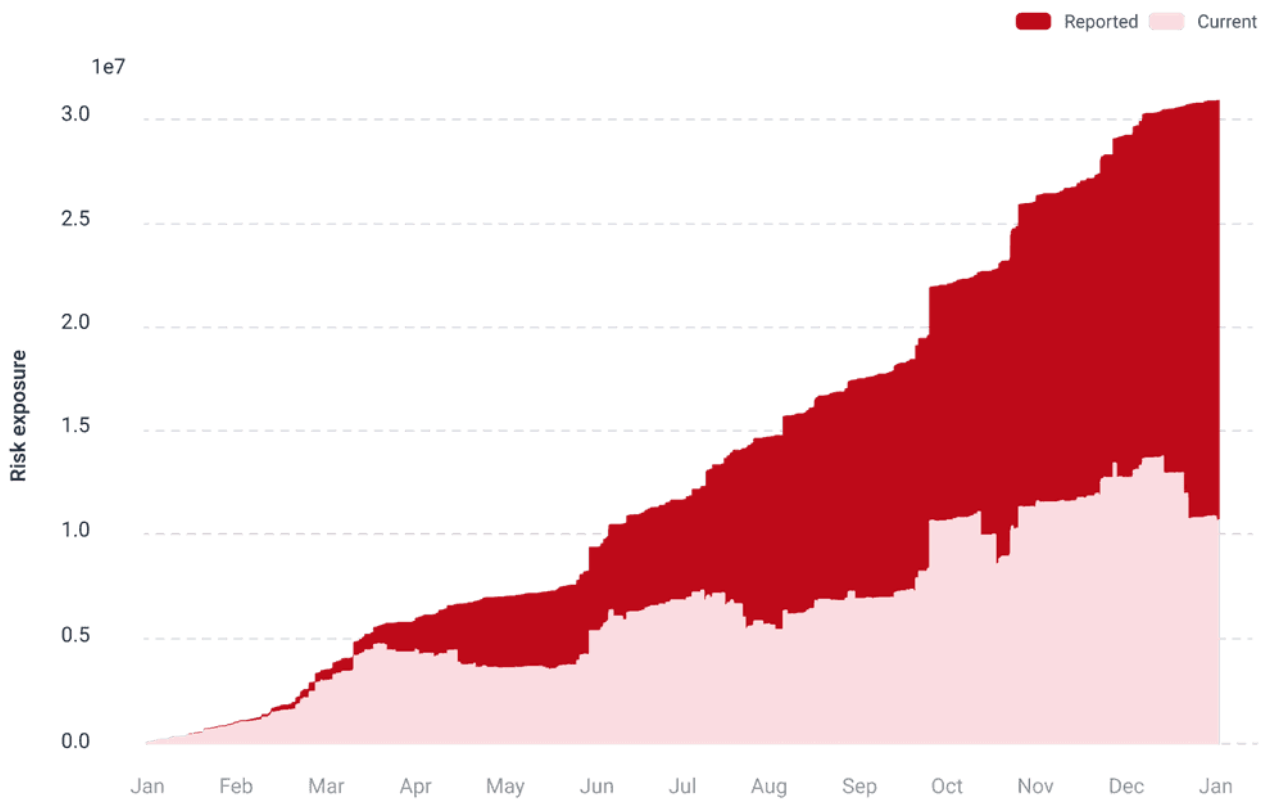
The latter average remediation rate was exceeded by the cumulative rates of seven months, which achieved a mean of **64.3%**. It was the first three remediation rates of the year that had the greatest influence on the decline in this average (for example, none of the critical vulnerabilities identified in January were remediated at the end of that month). Finally, the medium- and high-severity ranges achieved average rates of **36.7%** and **38.9%**, respectively.




## Remediation rate over time

By risk exposure

While only 41.0% of all vulnerabilities were remediated, the overall reduction in risk exposure reached **65.3%** by the end of the year. The remaining risk exposure is significantly influenced by those high-risk vulnerabilities (with high CVSSF values) that were not remediated at the time of closing the data collection for this report (some of which may have been identified in the last few months). Critical- and high-severity vulnerabilities accounted for **42.3%** and **44.3%** of the final risk exposure (i.e., at the end of 2024), each of these severity ranges with more than **4.5 million CVSSF units**.



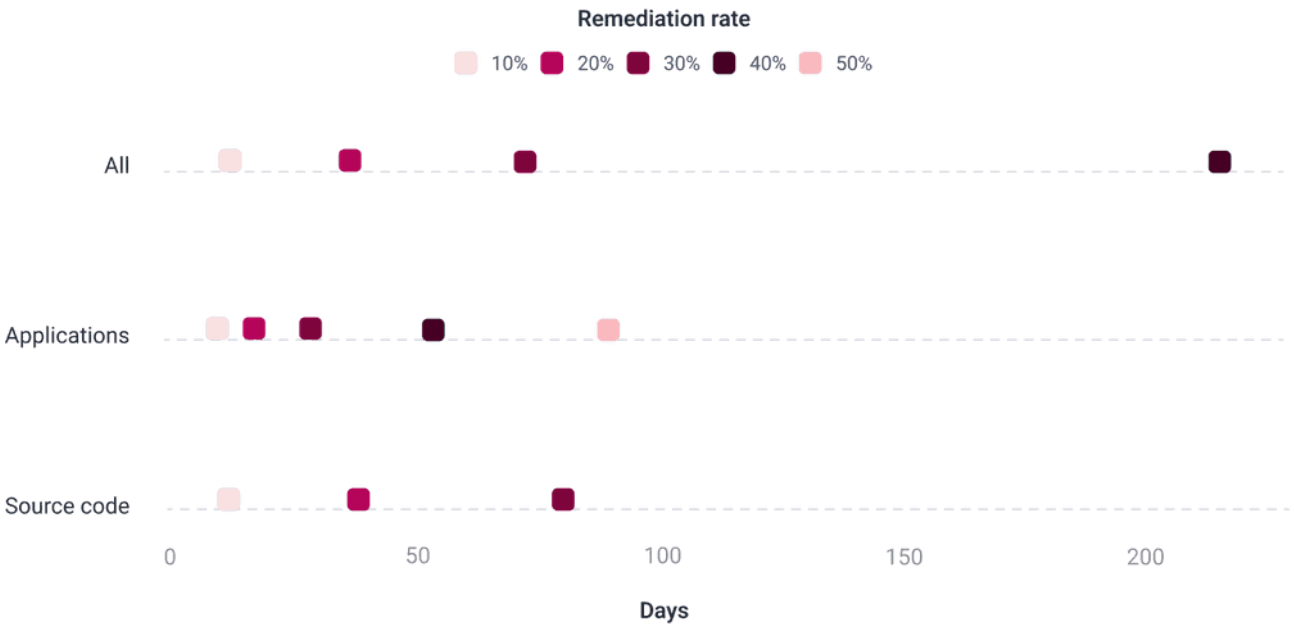

## Distribution of remediation rates

By target of evaluation

We arranged the vulnerabilities detected throughout the year according to their remediation time, starting with those fixed most quickly and ending with those that took the longest to remediate. After the latter, we added those that were not remediated, and then divided the entire data set into ten equal groups (i.e., deciles).

Notably, applications were the target with the **lowest 3rd decile**. In other words, 30% of vulnerabilities in running applications were fixed within 27 days, while the same percentage in source code was achieved just before 81 days. Furthermore, applications were **the only target where at least 50% of the vulnerabilities were remediated**, which was achieved in less than 90 days.

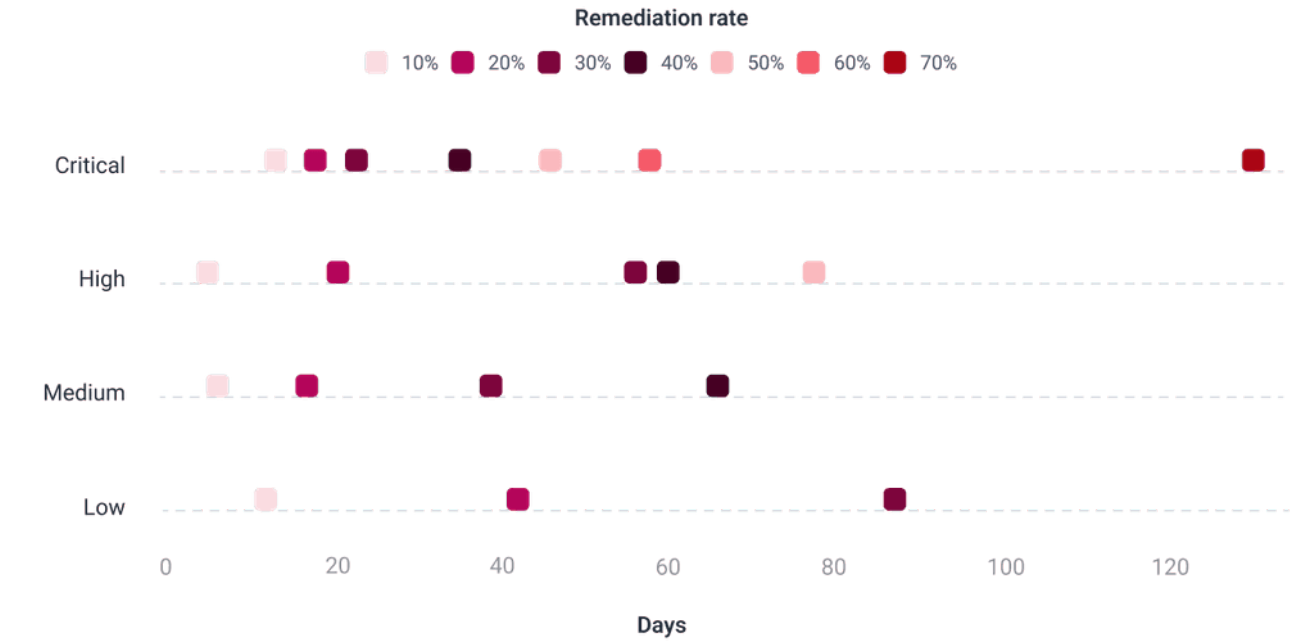
As mentioned above, very few vulnerabilities were reported for the infrastructures assessed, so this target of evaluation was not included in this analysis and does not appear in the following chart.




## Distribution of remediation rates

By severity

High- and critical-severity vulnerabilities were the only ones for which remediation rates exceeded **50%**. Even so, this **5th decile** was completed more promptly for critical-severity vulnerabilities, with fixes occurring in under **50 days**. Additionally, this was the only severity range to reach the **7th decile**. On the other hand, low-severity vulnerabilities ranked in the **3rd highest decile** and were the only range that did not reach a **40%** remediation rate by the end of 2024.



SECTION 07

## Vulnerability remediation support

Find out how much companies relied on the help of our experts

## 34.7%

/ Systems using Talk to a Pentester

At Fluid Attacks, we offer different support channels for vulnerability remediation. The main ones are**Autofix**,**Custom Fix**, and**Talk to a Pentester**. The first two are based on generative AI models and, within our IDE extensions and platform, automatically offer step-by-step guides and comprehensive remediation alternatives, respectively. The last channel, available only for the Advanced plan, provides the opportunity to schedule 30-minute virtual meetings with some of our pentesters to facilitate understanding of complex vulnerabilities.

Numerous organizations with software under assessment within Continuous Hacking's Advanced plan resorted to the **Talk to a Pentester** channel. Specifically, companies associated with **34.7%** of the systems (or groups) evaluated by our team of experts requested assistance sessions with them.

We invite you to take full advantage of this and the other support channels we offer, which can undoubtedly help you improve your remediation rates and times, thereby benefiting your organization's security posture.