ATLASSIAN

Bug bounty annual report

July 2022 - June 2023

Table of contents

This report summarizes the results for Atlassian's bug bounty program for Atlassian's financial year – July 1, 2022 through to June 30, 2023 (FY23). This includes a look at the results of the program across a range of metrics that are product, vulnerability, and payment based. Since we began our bug bounty program in 2017, it has been a fundamental cornerstone of our security assurance process for discovering and addressing vulnerabilities in our products.

Notable developments

Expanded scope of report

This year we have expanded the scope of this report to include three more of our products:

- Atlas
- Bamboo
- Compass

Updated data tracking

Utilising the connection between the data provided from our bug bounty and our internal vulnerability management dashboards, we were able to produce a dashboard that provides a level of granularity that was not available for previous reports.

All reports submitted through our bug bounty program undergo an additional level of verification and triage by our engineers, who have a deep understanding of our infrastructure and environment, before being included in our internal vulnerability management dashboards.

This increased scrutiny of the data and underlying root cause of vulnerabilities has resulted in lower overall numbers (for reference, FY23 has a 30% decrease from FY22 in the total number of reports). However, has created more actionable and auditable data as we are now only reporting on the reports that have been triaged into our internal vulnerability management dashboard (this includes reports that had both a payout and no payout).

Please refer to **Atlassian Vulnerability Management** for more information on how we track vulnerabilities internally.

Expansion of Atlassian's security testing capability

Security testing efforts at Atlassian have seen a significant increase over the past year. The Security Testing team is working closely with cyber security consultancies to conduct thorough penetration tests on Atlassian products.

This approach ensures that Atlassian's products and services undergo rigorous testing and evaluation. By combining the bug bounty program with the efforts by our security testing team, Atlassian can leverage the expertise of external researchers while also maintaining a proactive and comprehensive security posture.

This expansion in Security Testing has proven to be highly effective for Atlassian. The program's success is likely one of the factors contributing to the observed 30% decrease in bug bounty submissions during this financial year.

You can read more about these efforts at **Approach to External Security Testing** where additionally we publish "**Letters of Assessment**" for the annual penetration tests performed on Atlassian products.

Increased bounty payments in FY24

Atlassian is committed to enhancing and expanding our technical security assurance programs. This includes implementing more focused Bug Bounty programs and incentivising security researchers to concentrate on higher-risk areas in our products. As an example, from November to December 2023, we offered a 5x rewards multiplier for critical vulnerabilities (CVSS score 9.0+) for Confluence DC, which led to an increase in submissions and resulted in a more secure product.

Bug bounty results for our last fiscal year

Scope of report

Below we go into more detail around the results from our bug bounty program for the last financial year. The scope of the data we've included is focused on the following Atlassian products:

- Atlas
- Bamboo
- Bitbucket
- Compass
- Confluence
- Halp
- Jira Align
- Jira Software
- Jira Service Management
- Jira Work Management
- Opsgenie
- Statuspage
- Trello
- Automation for Jira
- Ecosystem
- Identity

In the July 2022 - June 2023 time-frame, Atlassian received a total of 251 valid vulnerability reports via our bug bounty program (from 79 unique researchers) which resulted in a payment for the products listed above. In the preceding year, Atlassian received a total of 358 valid vulnerability reports, which represents a 30% decrease year-over-year. Roughly 23% of the reports received were paid out, with roughly 77% of reports being unpaid reports.[1]

The remainder of this paper focuses on the data around these vulnerability reports.

We also saw an overall decrease in total vulnerabilities reports across all our bug bounties by 36% year–over-year, from 3,266 in FY22 to 2,076 in FY23.

Any security vulnerabilities identified from our bug bounty program are tracked in our internal Jira as they come through the intake process and will be triaged and remediated according to our **Security Bug Fix Policy**.

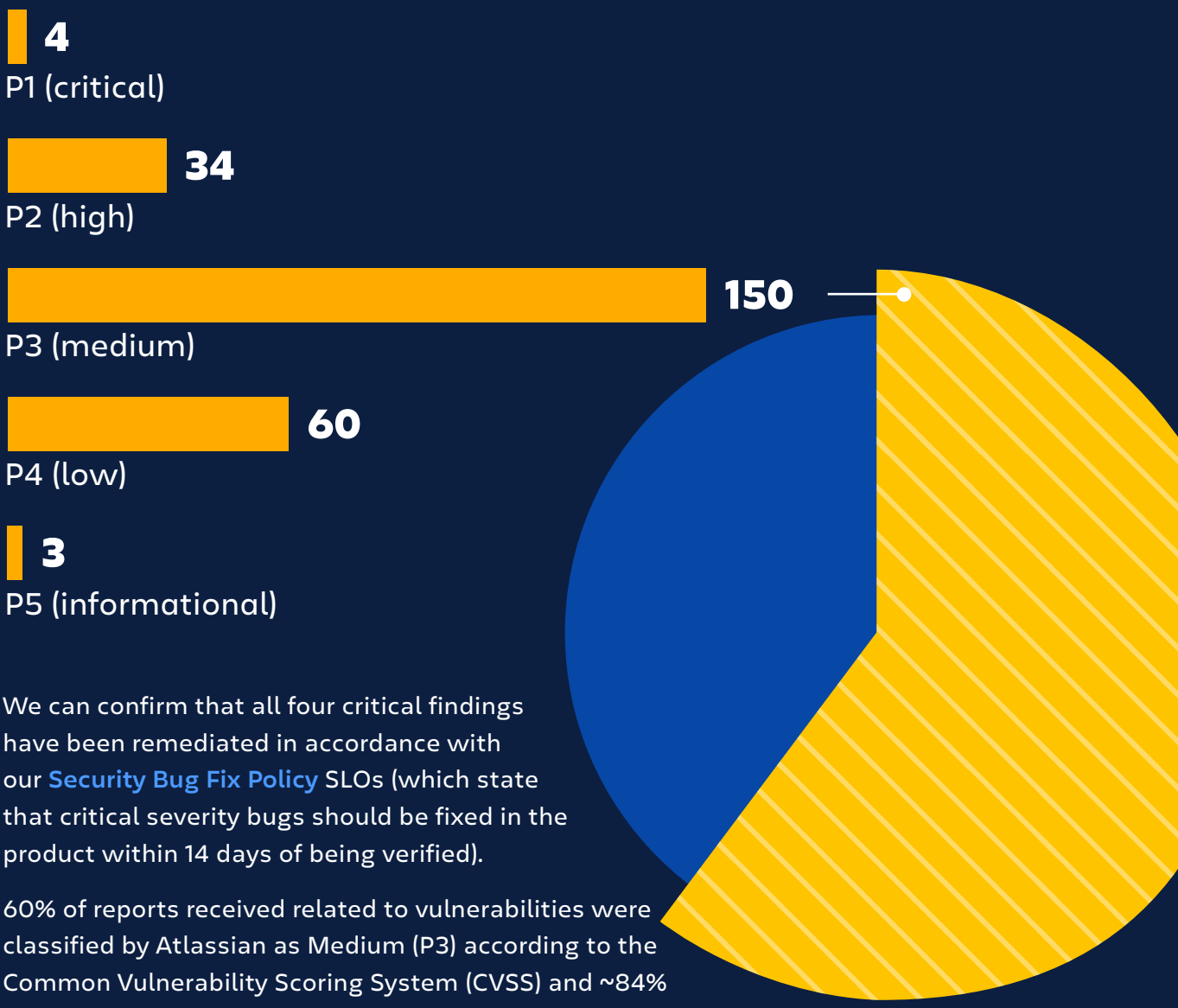
1. A reported vulnerability may not result in a payment for a range of reasons, including it not being reproducible by Atlassian, outside the scope of the program, a duplicate of a vulnerability already reported, or real but not entitled to a bounty payment (for example, because the bug is real but gives no advantage to a potential attacker).

Vulnerability reports by CVSS severity level

The following graph displays the count of valid low, medium, high, and critical vulnerabilities that were reported to Atlassian through the bug bounty program for the products in-scope.

60% of reports were classified as Medium

VULNERABILITY REPORTS BY CVSS SEVERITY LEVEL



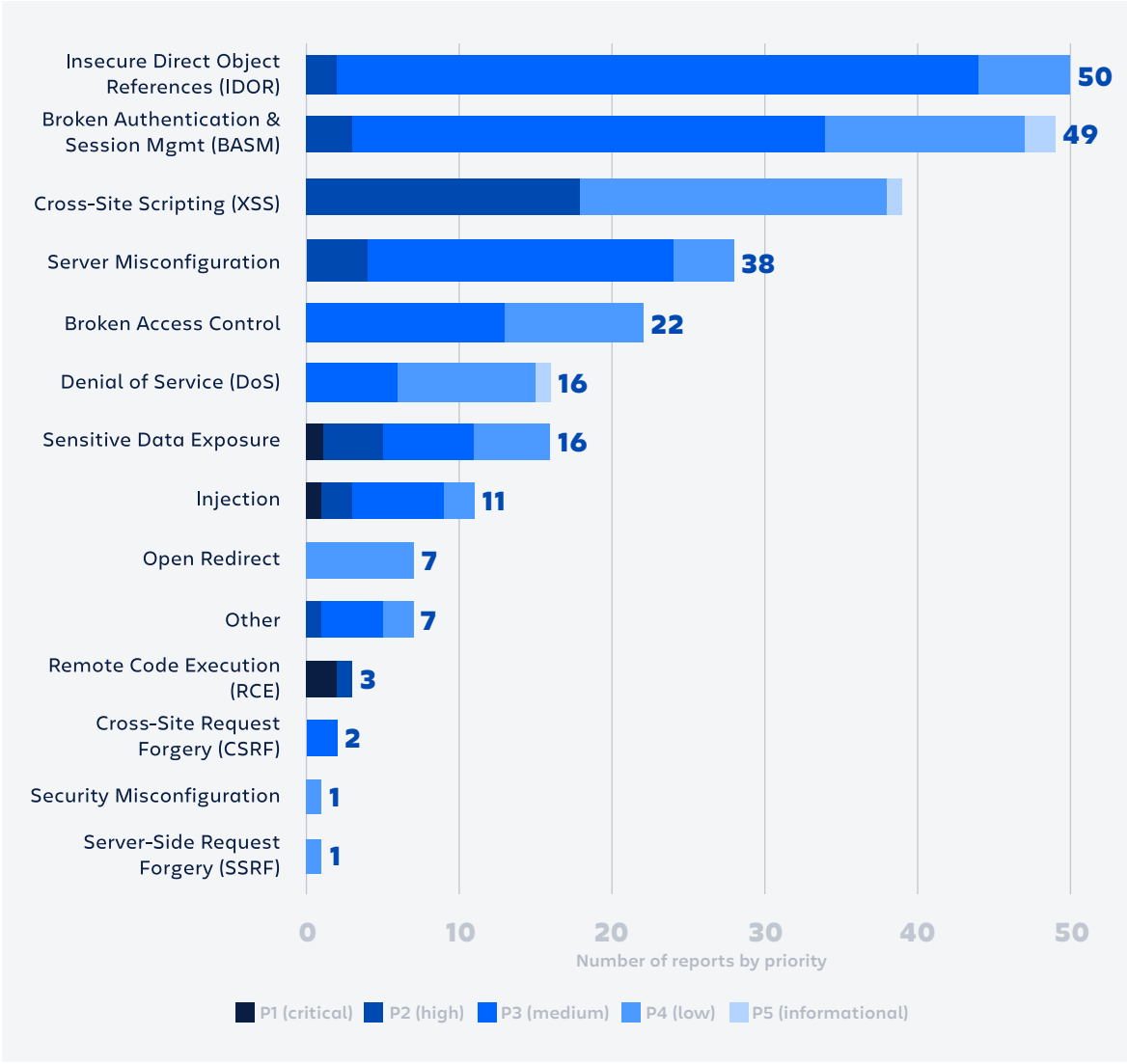
We can confirm that all four critical findings have been remediated in accordance with our Security Bug Fix Policy SLOs (which state that critical severity bugs should be fixed in the product within 14 days of being verified).

60% of reports received related to vulnerabilities were classified by Atlassian as Medium (P3) according to the Common Vulnerability Scoring System (CVSS) and ~84% of all vulnerabilities were Medium (P3) or Low (P4).

Vulnerability reports by type

The graph below outlines the types of vulnerabilities that were most frequently reported to Atlassian. Insecure Direct Object References (IDOR) related issues were the most frequently reported type of vulnerabilities, with 50 reports. Broken Authentication and Session Management (BASM) followed closely behind with 49 reports. These two categories combined accounted for 39.4% of the total reported vulnerabilities in the bug bounty program.

We have also updated our visualisation this year to provide our customers with a more in-depth view of the priority level at which our bug types usually fall.



In FY22, we received 138 valid BASM vulnerabilities, and in FY23, we received 49 valid BASM vulnerabilities, representing a decrease of 64%.

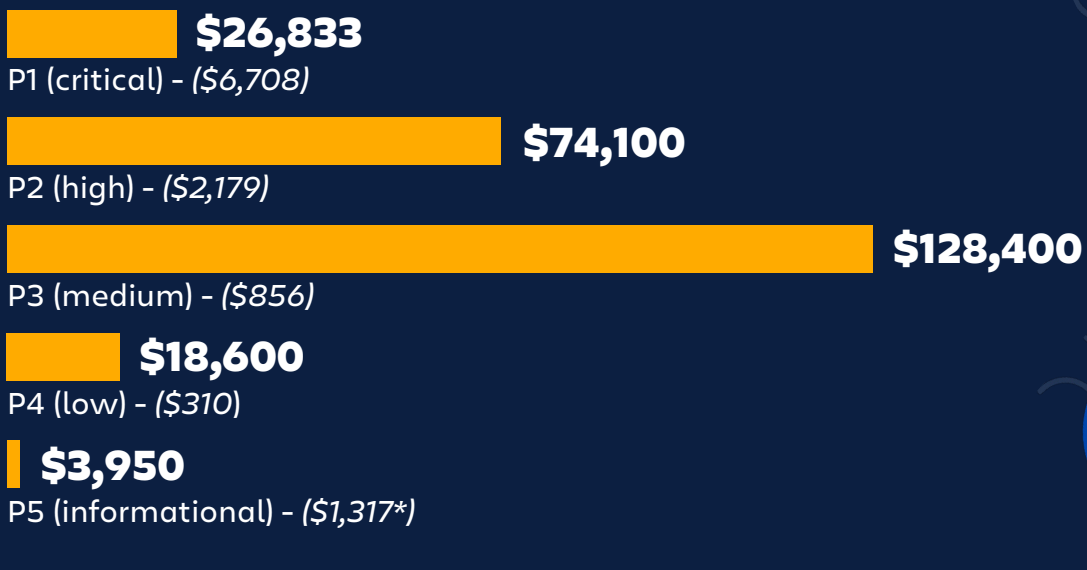
Bounty payments by CVSS severity level

In our last financial year, Atlassian made a total of $251,883 (USD) worth of payments via its bug bounty program for the products in-scope for this paper. The highest cumulative payments were for vulnerabilities that fell into the medium (P3) severity level, at $128,400, and high (P2) severity level, at $74,100. In our preceding year, Atlassian made a total of $383,600 worth of payments, which represents a ~34% decrease in payments for the FY23 financial year (this decrease in payments comes as a direct result of the decrease in the number of reports).

It is important to note that the amount of payment for individual bugs will vary based not only on the CVSS severity level, but also which product the report applies to (critical reports for our Tier 1 products for example will pay higher than a critical report for a Tier 2 or Tier 3 product). Average payout per severity is noted in parenthesis.

Atlassian made $251,883 worth of total payments via its bug bounty program

TOTAL PAYMENTS BY CVSS SEVERITY LEVEL ($USD)



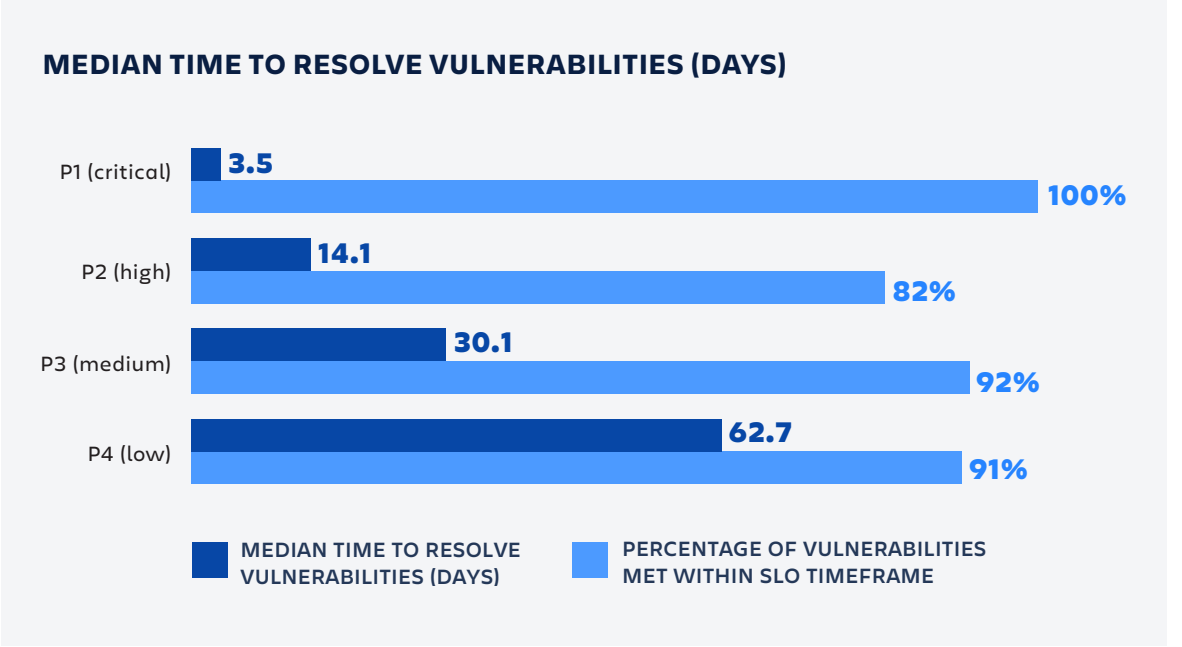
*Informational reports that had a pay-out came as a result of reports that were initially categorised in a higher category and paid out, which were then recategorised to Informational upon further review. There is typically no pay-out for reports that are initially categorised as Informational.

Bounty payments by vulnerability type

In the graph below we break down the total bounty payments Atlassian made for each vulnerability type, taking into account CVSS severity level and product tier. It is important to note that in some instances, the higher CVSS level of reported vulnerabilities resulted in a higher total payout to researchers for particular categories, even when those categories may have had less total reports for the financial year than others.

Time to resolve reported vulnerabilities by CVSS severity level

The graph and data below indicates the median time, in days, Atlassian took to resolve vulnerabilities reported to it via the bug bounty program.



As a point of comparison, Atlassian's SLOs for different vulnerability types (as per our Security Bug Fix Policy) are listed below:

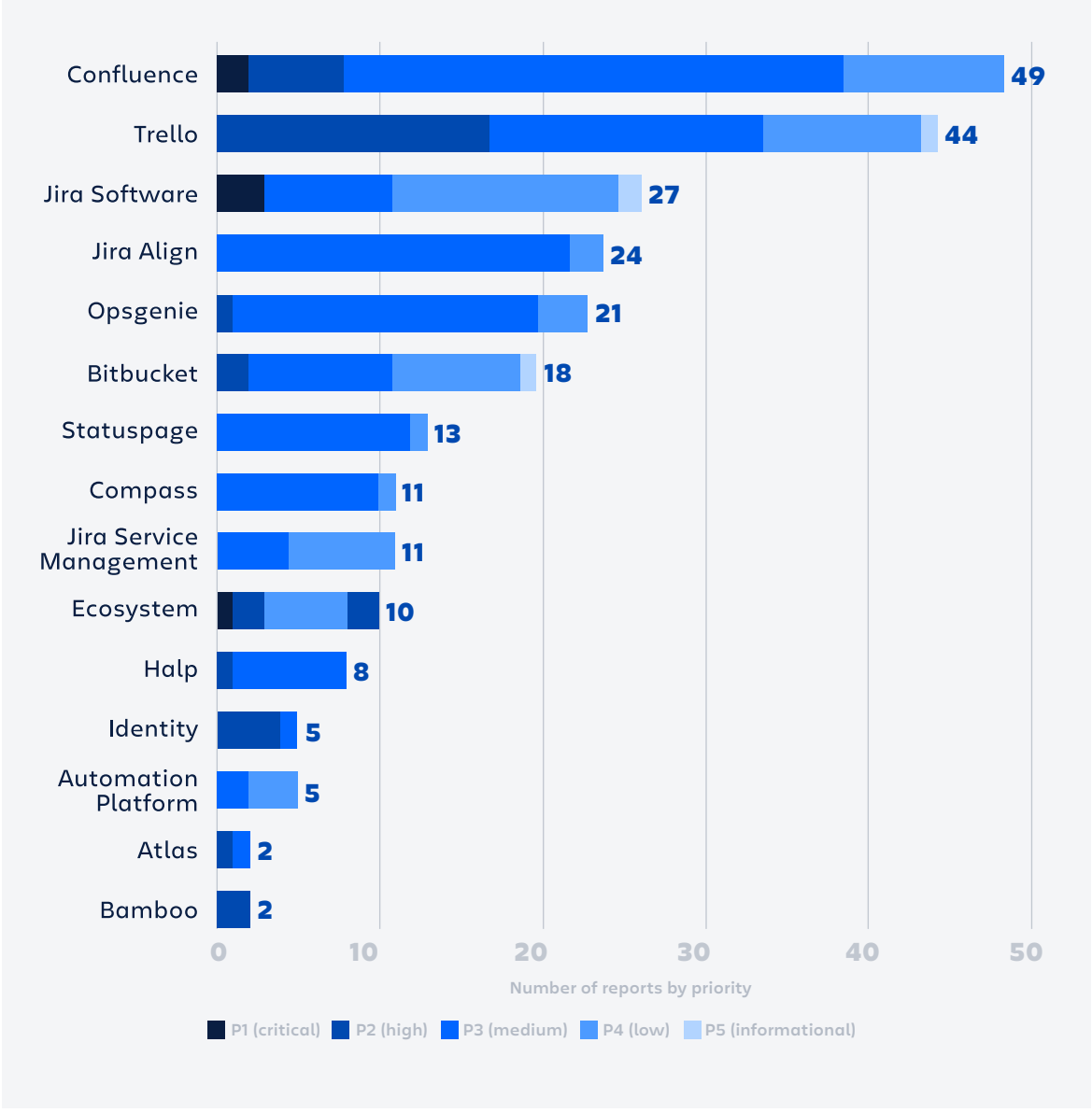
- **Critical** severity bugs to be fixed in product within two weeks of being verified
- **High severity** bugs to be fixed in product within four weeks of being verified
- **Medium severity** bugs to be fixed in product within six weeks of being verified
- **Low severity** bugs to be fixed in product within 25 weeks of being verified

For all vulnerability severities, the median time to resolve vulnerabilities were less than the current SLO.

Vulnerability reports by product

This graph covers the number of valid vulnerabilities reported for each product during the July 2022 – June 2023 (FY23) period for which a payment was made. Confluence Cloud had the largest number of reported vulnerabilities for which payments were made (49), followed by Trello (44), Jira Software (27) and Jira Align (24). Jira Work Management had the least number of valid vulnerability reports at zero.

We have also updated our visualisation this year to provide our customers with a more in-depth view of the priority level at which our bug types usually fall for each product.



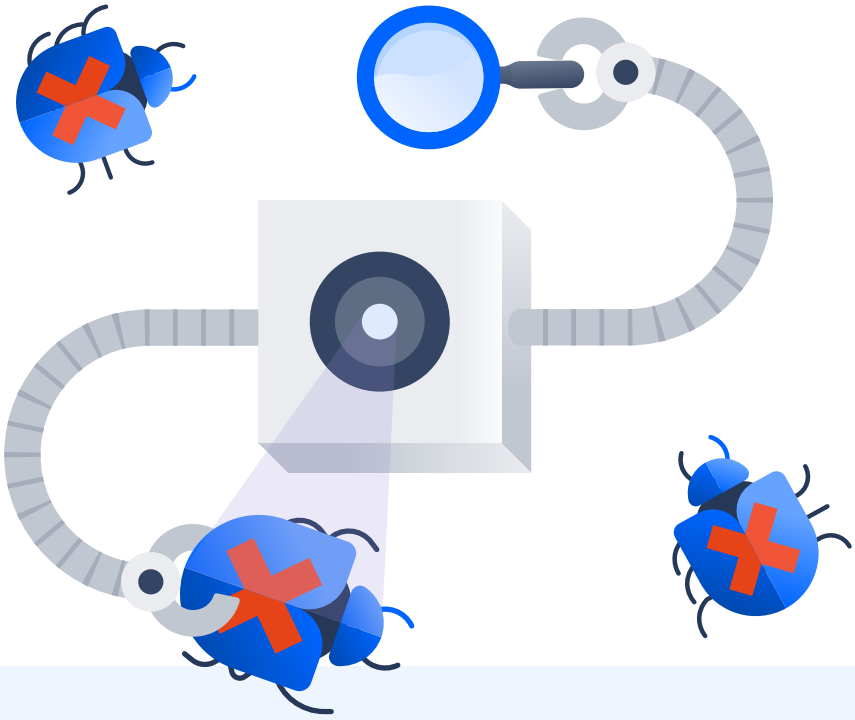
Bounty payments by product

In the graph below, we break down the total bounty payments made by product. Confluence Cloud had the highest cumulative payout ($92,600), followed by Jira Software ($40,150), Trello ($30,733) and Opsgenie ($23,100).

More information

If you need more information about Atlassian's bug bounty program, approach to security testing, or security program more generally, you can check out the following resources:

- Our Approach to External Security Testing
- Our Security Bug Fix Policy
- The Atlassian Trust Center



You can also contact Atlassian's Trust Team, via our support portal if you still need further clarification on anything to do with this paper or our approach to security generally. Alternatively, ask a question in our Atlassian Trust and Security Community.

ATLASSIAN