ATLASSIAN

Bug bounty annual report

July 2021 - July 2022

Table of contents

This report summarizes the results for Atlassian's bug bounty program for Atlassian's financial year – July 1, 2021 through to June 30, 2022 (FY22). 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 partnering with Bugcrowd on a full-time basis in 2017, Atlassian's bug bounty program has been a fundamental cornerstone of our security assurance process for discovering and addressing vulnerabilities in our products. It has consistently been recognised as one of the best in the industry, and enables us to leverage a trusted community of tens of thousands of security researchers.

Notable developments in the bug bounty program

Increased bounty payments

In the last 12 months, Atlassian increased the bounty payments for valid vulnerabilities identified via our bug bounty program. This included:

- Doubling payments for critical and high severity vulnerabilities[1] identified for our core cloud products (Bitbucket, Confluence, Jira and Trello)
- Increasing the payments for our other product tiers as well.

Current payments to Bugcrowd researchers for reported vulnerabilities – by tier and CVSS Severity Level – are captured in the table below. The previous payment amount is listed in parenthesis next to each current payment amount.

Payout by Product Tier ($USD)

Severity level	Tier 1	Tier 2	Tier 3
Critical (P1)	$10,000 ($5,000)	$6,000 ($3,000)	$4,000 ($1,500)
High (P2)	$3,600 ($1,800)	$2,400 ($900)	$1,200 ($900)
Medium (P3)	$1,200 ($600)	$800 ($300)	$500 ($300)
Low (P4)	$300 ($200)	$300 ($100)	$200 ($100)

1. Based on the **Common Vulnerability Scoring System (CVSS)**

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 Cloud products:

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

In the July 2021 - June 2022 time-frame, Atlassian received a total of 358 valid vulnerability reports via our bug bounty program which resulted in a payment[2] for the products listed above. In the preceding year, Atlassian received a total of 348 valid vulnerability reports, which represents a ~3% increase year-over-year. The remainder of this paper focuses on the data around these vulnerability reports.

We also saw an overall increase in total vulnerabilities reports by 11% year–over-year, from 2,950 in FY21 to 3,266 in FY22.

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 **Public Security Vulnerability SLA**.

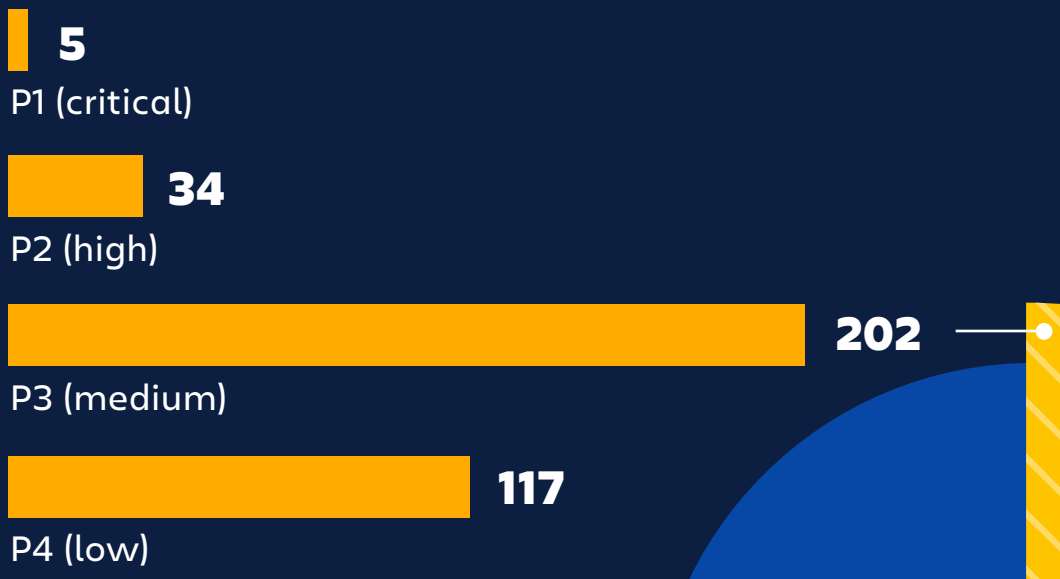
2. A reported vulnerability may not result in a payment for a range of reasons, including it not being reproducible by Atlassian, outside the scope of the program, a duplicate of a vulnerability already reported, or real but not entitled to a bounty payment (for example, because the bug is real but gives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

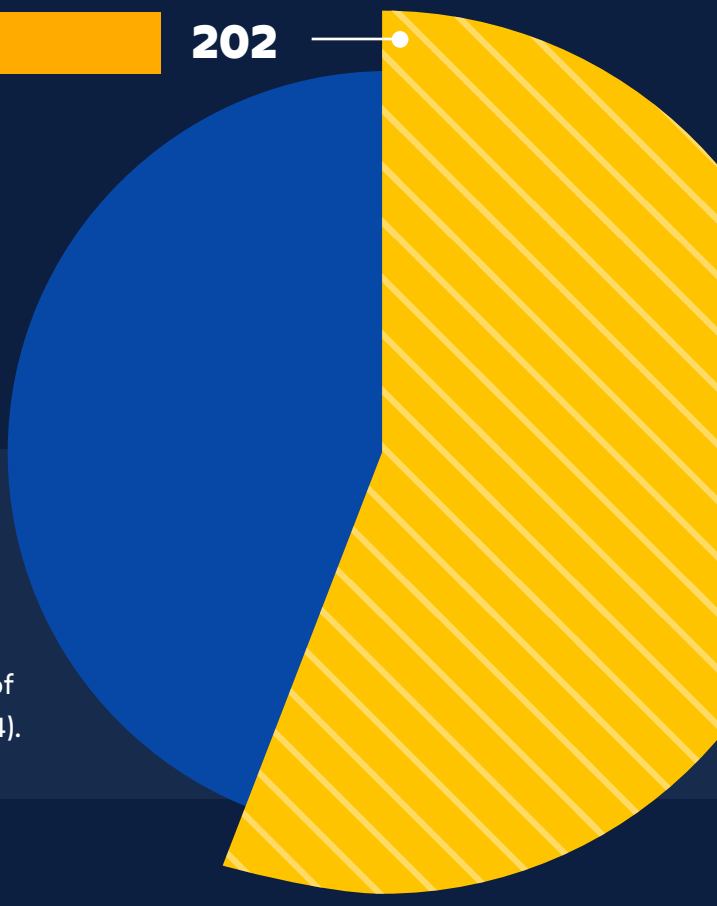
Vulnerability reports by CVSS severity level

Below is shown the number of valid low, medium, high and critical vulnerabilities reported to Atlassian via the bug bounty program across the products in-scope for this report.

56% of reports were classified as Medium

VULNERABILITY REPORTS BY CVSS SEVERITY LEVEL

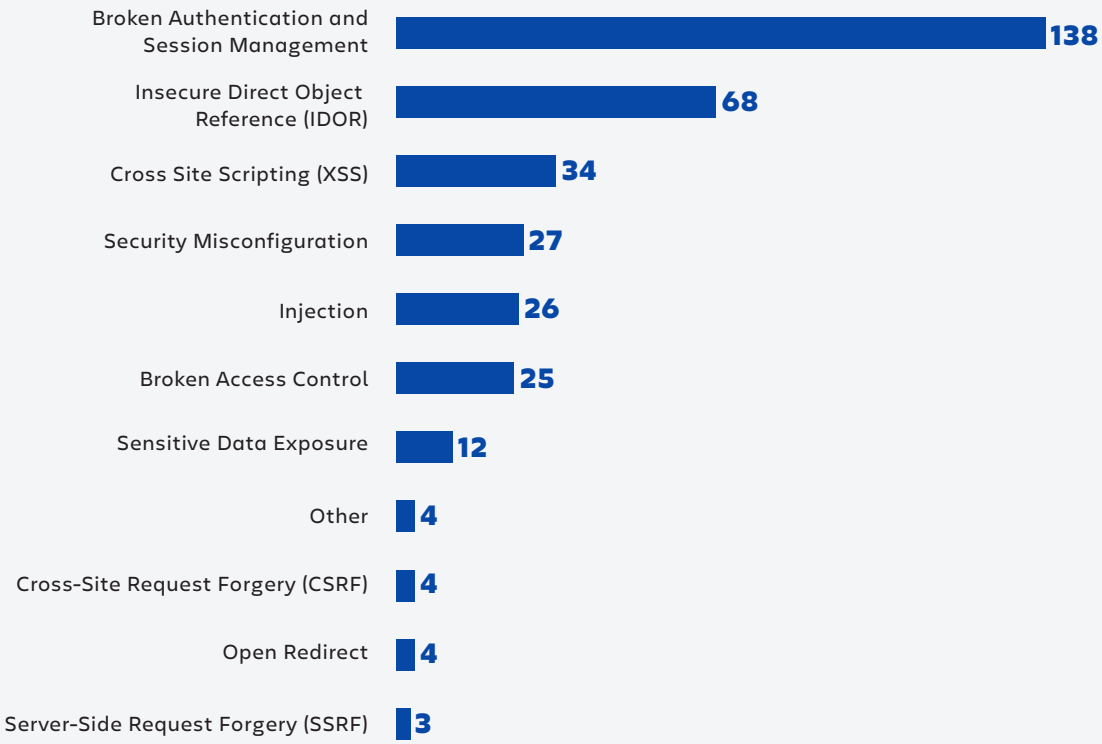




56% of reports received related to vulnerabilities were classified by Atlassian as Medium (P3) according to the Common Vulnerability Scoring System (CVSS) and 89% of all vulnerabilities were Medium (P3) or Low (P4).

Vulnerability reports by type

The graph below[3] outlines the types of vulnerabilities that were most frequently reported to Atlassian. Broken Authentication and Session Management (BASM) related issues were the most frequently reported through the bug bounty, accounting for 38% of total reported vulnerabilities.



In FY22, Atlassian received a significant number of low severity reports regarding Broken Authentication & Session Management (BASM) vulnerabilities from a small set of researchers. Many of these particular submissions' reports are similar in technique, with the only material difference between them being the resource requested.

In FY21, we received 98 valid XSS vulnerabilities, and in FY22, we received 34 valid XSS vulnerabilities, or a reduction of 66%. Similar to the BASM explanation above, in FY21, the Jira Platform received ~20 XSS submissions that were all very similar in nature and technique, but we paid out independently as they required distinct locations to fix in the code base.

3. There were a small number of vulnerability categories that had only had one report. These have not been included in the graph.

Bounty payments by CVSS severity level

In our last financial year, Atlassian made a total of $ 383,600 (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 $195,700, and high (P2) severity level, at $113,600. In our preceding year, Atlassian made a total of $258,350 worth of payments, which represents a ~48% increase in payments for this financial year, due to the increase in payouts per severity in May 2021.

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 $383,600 worth of total payments via its bug bounty program

TOTAL PAYMENTS BY CVSS SEVERITY LEVEL ($USD)

P1 (critical) – *($8000)*

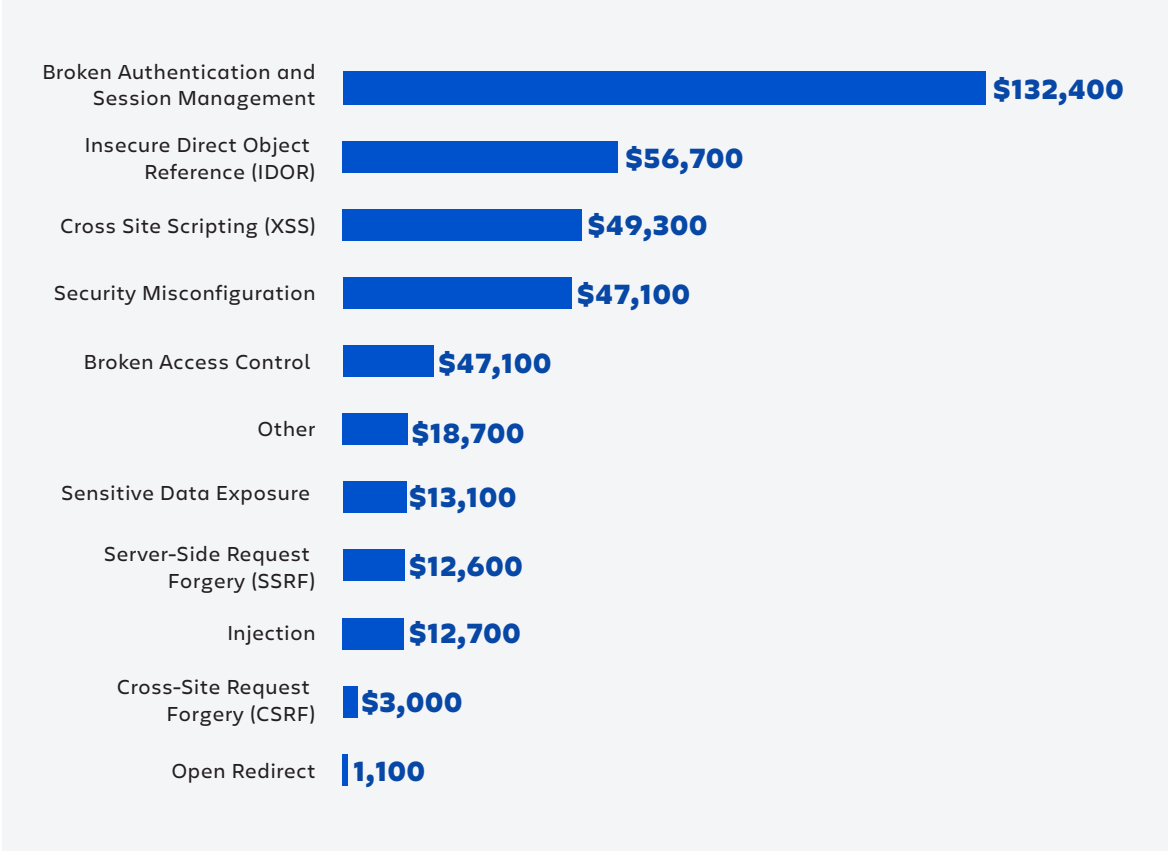
P2 (high) – *($3,340)*

P3 (medium) – *($969)*

P4 (low) – *($293)*

Bounty payments by vulnerability type

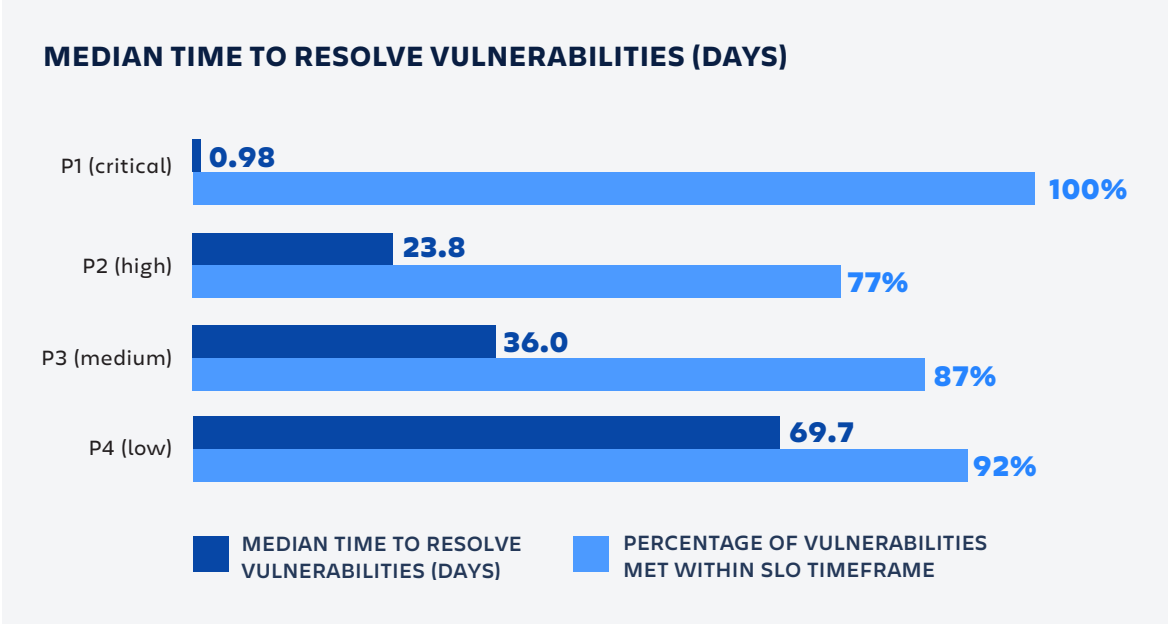
In the graph below we break down the total bounty payments Atlassian made for each vulnerability type, taking into account CVSS severity level and product tier. It is important to note that in some instances, the higher CVSS level of reported vulnerabilities resulted in a higher total payout to researchers for particular categories, even when those categories may have had less total reports for the financial year than others (for example, injection related vulnerabilities were more frequently reported than those related to server misconfigurations, however the latter category had a higher total payout by almost $25,000 USD).



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. We have used the median rather than mean time because there were some distortions in the data that arose by a small number of vulnerabilities that were 'outliers' in terms of resolution time for various reasons, which distorts the mean figure.

All Critical (P1) vulnerabilities were fixed well within SLO, with a median timeframe of one day.



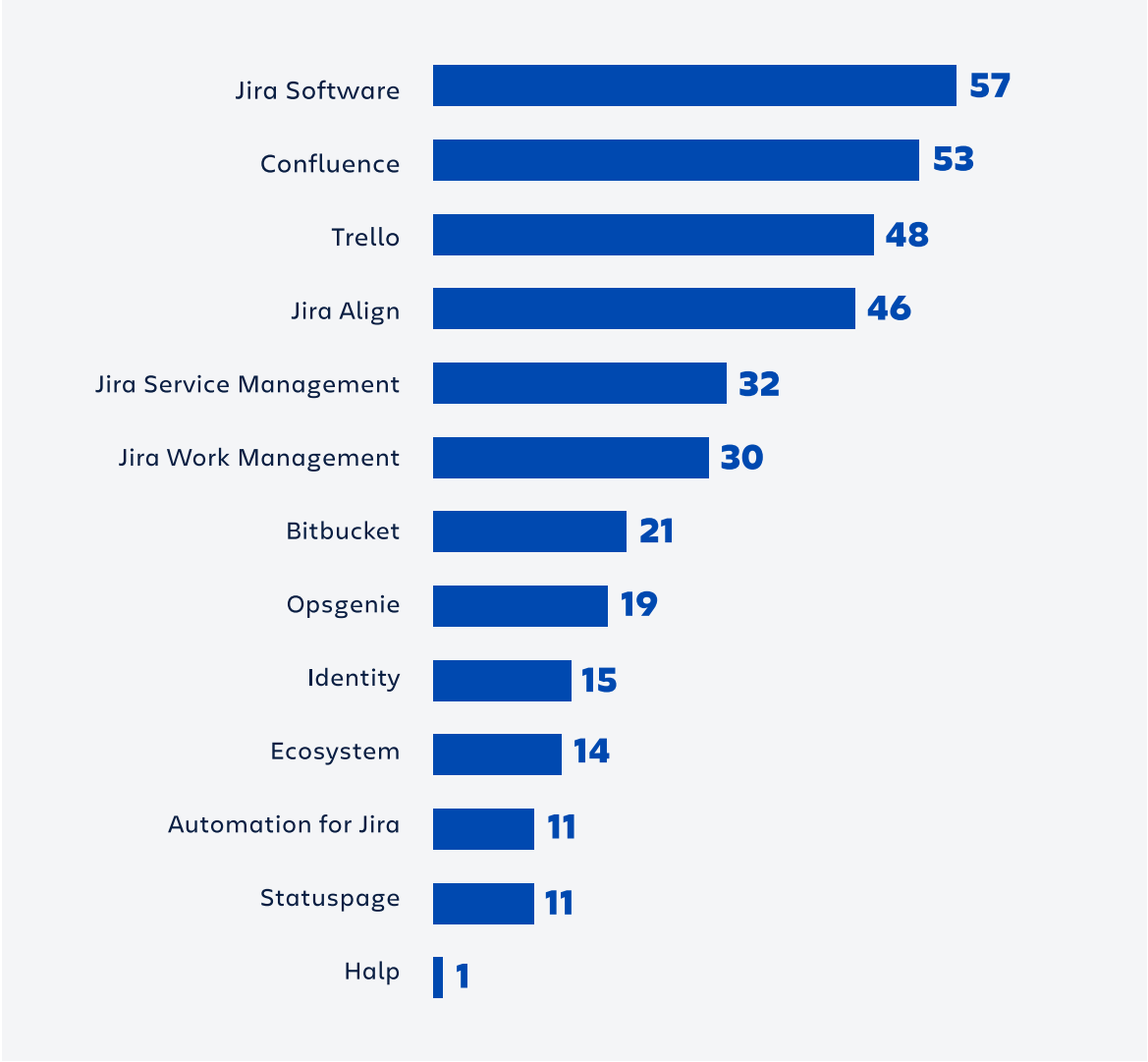
As a point of comparison, Atlassian's SLOs for different vulnerability types (as per our Security Bug Fix Policy) are listed below:

- P1 (Critical) - **14 days**
- P2 (High) - **28 days**
- P3 (Medium) - **42 days**
- P4 (Low) - **175 days**

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

Vulnerability reports by product

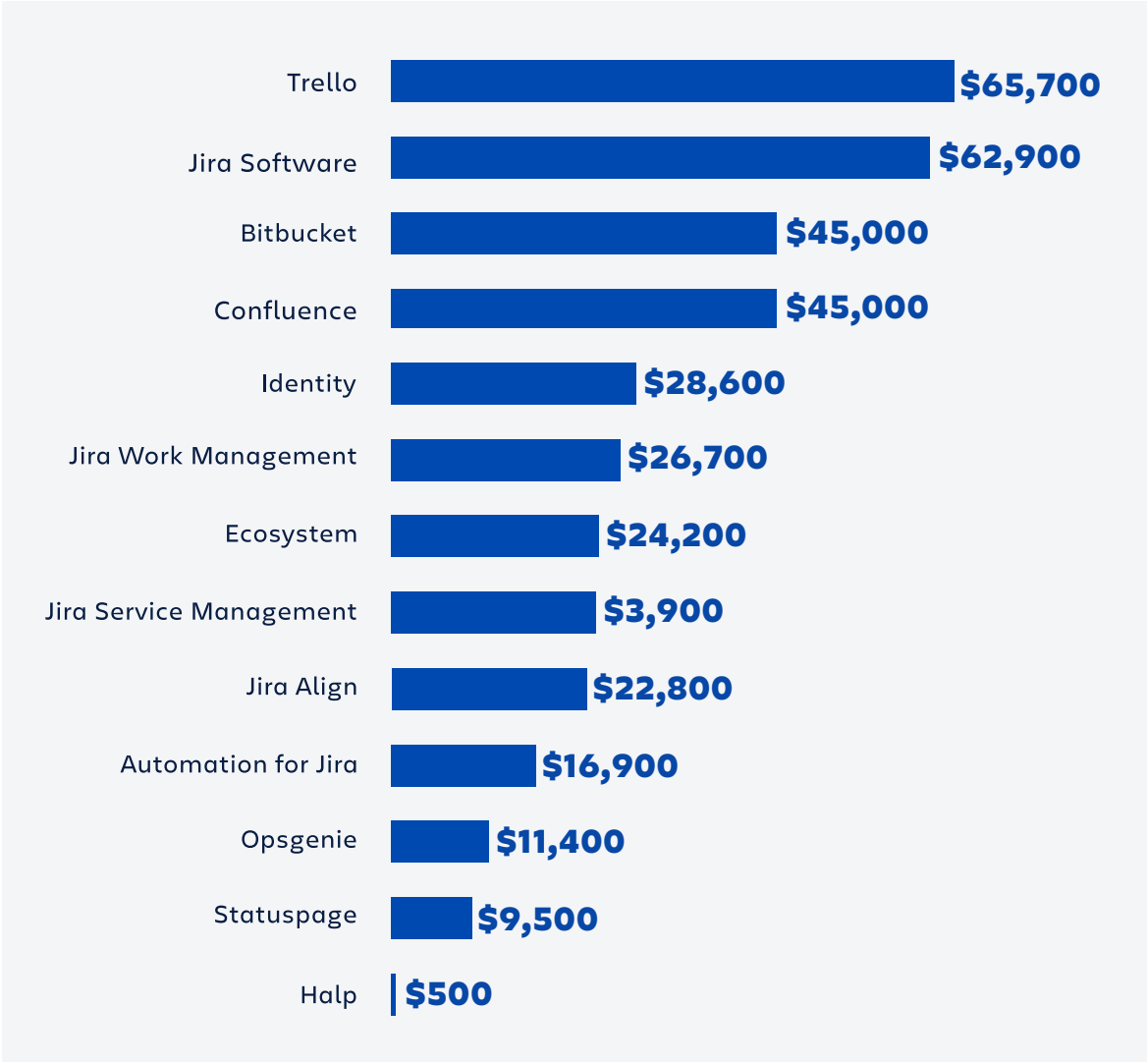
This graph covers the number of valid vulnerabilities reported for each product during the July 2021 – June 2022 (FY22) for which a payment was made. Jira Software had the largest number of reported vulnerabilities for which payments were made (57), followed by Confluence (53), Trello (48) and Jira Align (46). Halp had the least number of valid vulnerability reports, at just one.



In FY21, we ran a targeted Bug Bounty Blitz at Trello and Trello Power-Ups. While Trello had the most valid vulnerabilities in FY21 (98), Trello saw a reduction of ~50% of valid vulnerabilities in FY22 (48).

Bounty payments by product

In the graph below, we break down the total bounty payments made by product. Trello had the highest cumulative payout ($65,700), followed closely by Jira Software ($62,900), Bitbucket ($45,000) and Confluence ($45,000).



Number of reports by researcher

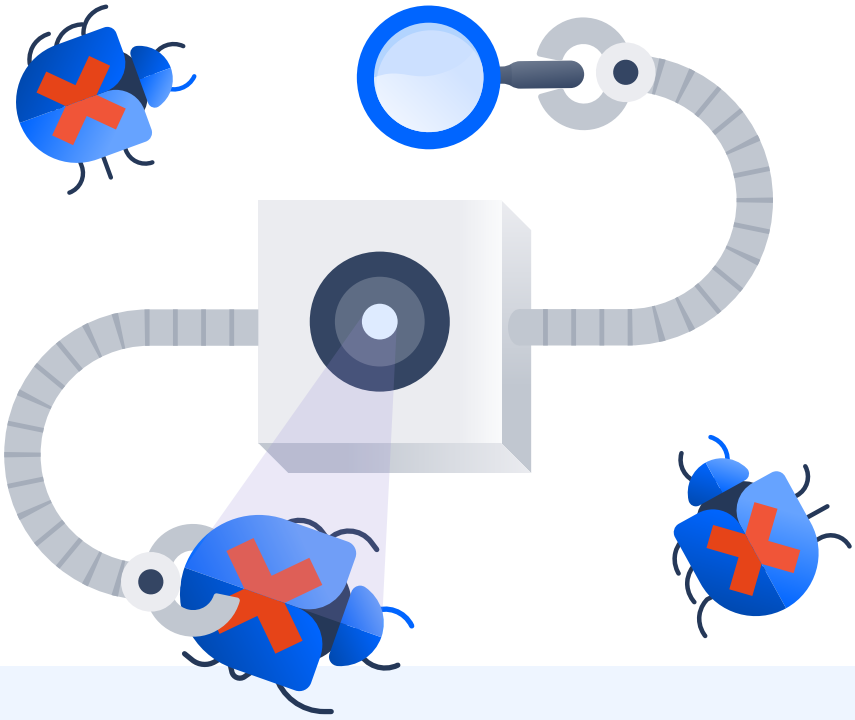
Our bug bounty program has several contributing researchers. Below, we list the top 15 contributors (by number of vulnerabilities reported) for the program for the last financial year. The contributions of all our researchers, no matter the number of reports submitted, is highly valued. Their details can be found in the **Atlassian Bug Bounty Hall of Fame**, the **Opsgenie Bug Bounty Hall of Fame**, the **Statuspage Bug Bounty Hall of Fame**, and the **Trello Bug Bounty Hall of Fame**.

Researcher	Number of vulnerabilities reported
MrHack	63
UpdateLap	39
d0xing	26
theflofly	25
AnkitSingh	19
Labda	18
Hx01	17
toukakirishima	13
Lethal	13
Imran_Nazir	13
l0gg	12
Sarah Haver	10
randrly	10
Mr_sharma_	9
snapsec	8

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