



# Bug bounty annual report

July 2020 - July 2021



# Table of contents

<b>3</b>	<b>Introduction</b>
<b>4</b>	<b>Notable developments in the bug bounty program</b>
4	Increased bounty payments
5	Identifying bugs in Bitbucket Pipelines
<b>6</b>	<b>Bug bounty results for our last fiscal year</b>
6	Increased bounty payments
7	Vulnerability reports by CVSS severity level
8	Vulnerability reports by type
9	Bounty payments by CVSS severity level
10	Bounty payments by vulnerability type
11	Time to resolve reported vulnerabilities by CVSS severity level
12	Vulnerability reports by product
13	Bounty payments by product
14	Number of reports by researcher
15	Total payments by researcher

This paper summarizes the results for Atlassian's bug bounty program for the 2021 financial year (July 1, 2020 through to June 30, 2021). 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<sup>1</sup> 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 brackets next to each current payment amount.

## Payout by Product Tier (\$USD)

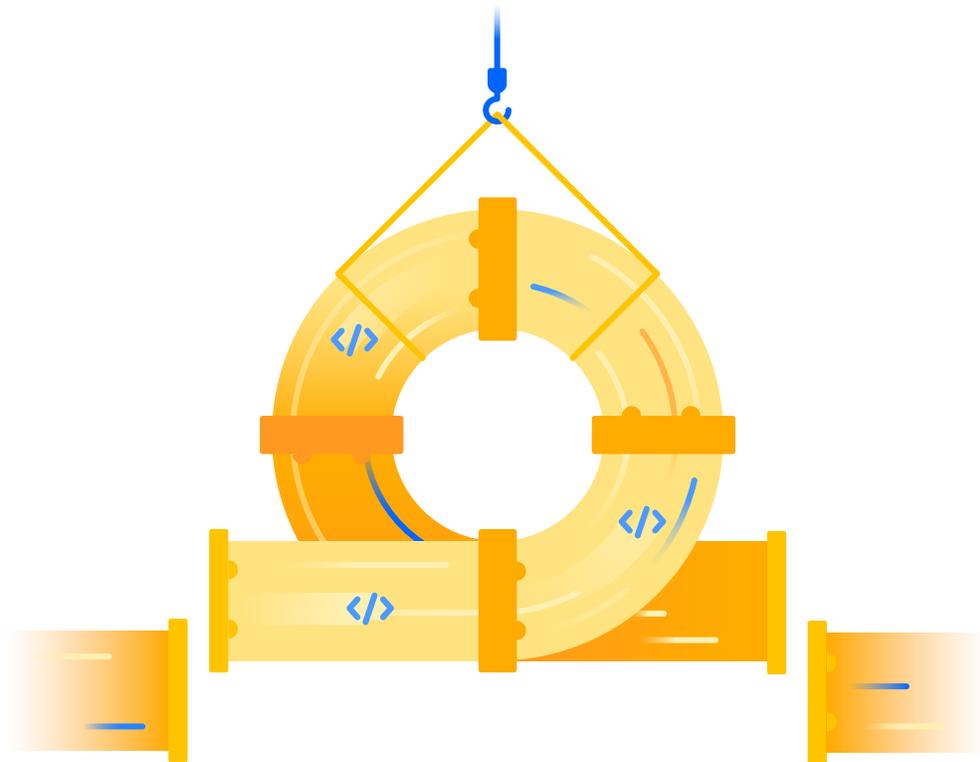
Severity level	Tier 1	Tier 2	Tier 3
Critical (P1)	\$10,000 (\$5,000)	\$6,000 (\$3,000)	\$4,000 (\$1,500)
High (P2)	\$3,600 (\$1,800)	\$2,400 (\$900)	\$1,200 (\$900)
Medium (P3)	\$1,200 (\$600)	\$800 (\$300)	\$500 (\$300)
Low (P4)	\$300 (\$200)	\$300 (\$100)	\$200 (\$100)

1. Based on the [Common Vulnerability Scoring System \(CVSS\)](#)

## Identifying bugs in Bitbucket Pipelines

Atlassian ran a special project via Bugcrowd to look for bugs in its planned implementation of Kata Containers within our Bitbucket Pipelines CI/CD environment. During the project, a researcher identified a significant vulnerability in Kata Containers which could potentially allow an attacker to assume root privileges on the pipeline host.

The vulnerability was then fixed by the Kata Containers team based on the information provided by the researcher. This case study provides a clear example of the value of Atlassian's bug bounty program to improving the security of its products (including where vulnerabilities may be introduced through the use of third party open source components in our products). More information about this project is [available from Bugcrowd](#).



# Bug bounty results for our last fiscal year

## Increased bounty payments

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 Cloud products:

-  Jira Align
-  Statuspage
-  Jira Service Management
-  Bitbucket
-  Jira Work Management
-  Opsgenie
-  Jira Software
-  Trello
-  Confluence

In the preceding financial year, Atlassian received a total of **348 vulnerability reports** via our bug bounty program which resulted in a payment<sup>2</sup> for the products listed above. The remainder of this paper focuses on the data around these reports.

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](#).

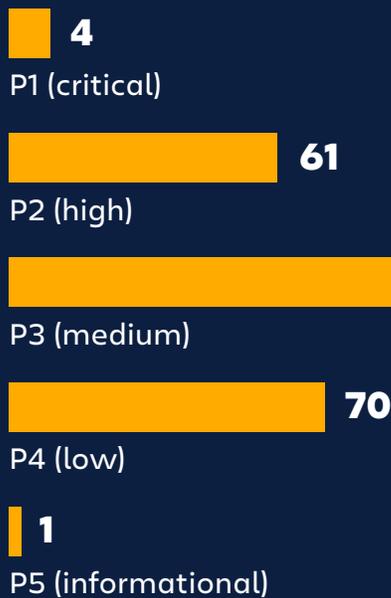
2. A reported vulnerability may not result in a payment for a range of reasons, including it not being reproducible by Atlassian, outside the scope of the program, a duplicate of a vulnerability already reported, or real but not entitled to a bounty payment (for example, because the bug is real but gives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

## Vulnerability reports by CVSS severity level

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

**61%** of reports were classified as Medium

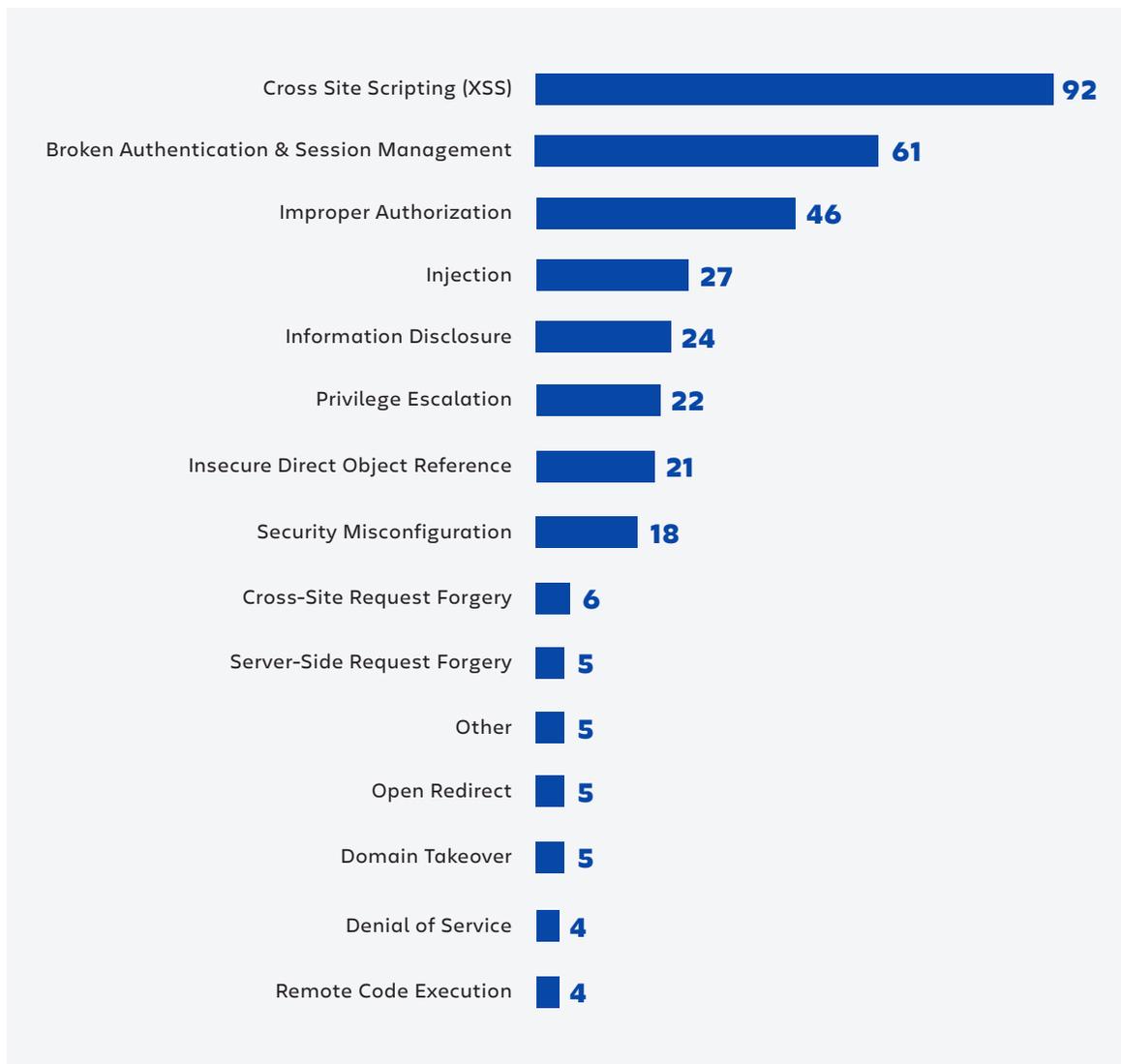
### VULNERABILITY REPORTS BY CVSS SEVERITY LEVEL



Close to two-thirds of reports received related to vulnerabilities were classified by Atlassian as Medium (P3) according to the Common Vulnerability Scoring System (CVSS).

## Vulnerability reports by type

The graph below<sup>3</sup> outlines the types of vulnerabilities that were most frequently reported to Atlassian. Cross site scripting related issues were the most frequently reported through the bug bounty, accounting for 26% of total reported vulnerabilities.



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

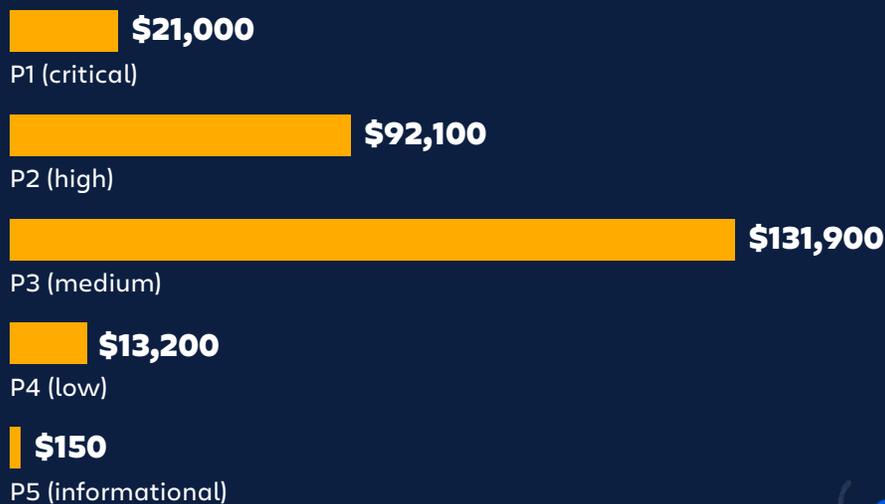
## Bounty payments by CVSS severity level

In the last financial year, Atlassian made a total of \$258,350 (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 \$131,900, and high (P2) severity level, at \$92,100.

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).

# Atlassian made **\$258,350** worth of total payments via its bug bounty program

### TOTAL PAYMENTS BY CVSS SEVERITY LEVEL (\$USD)



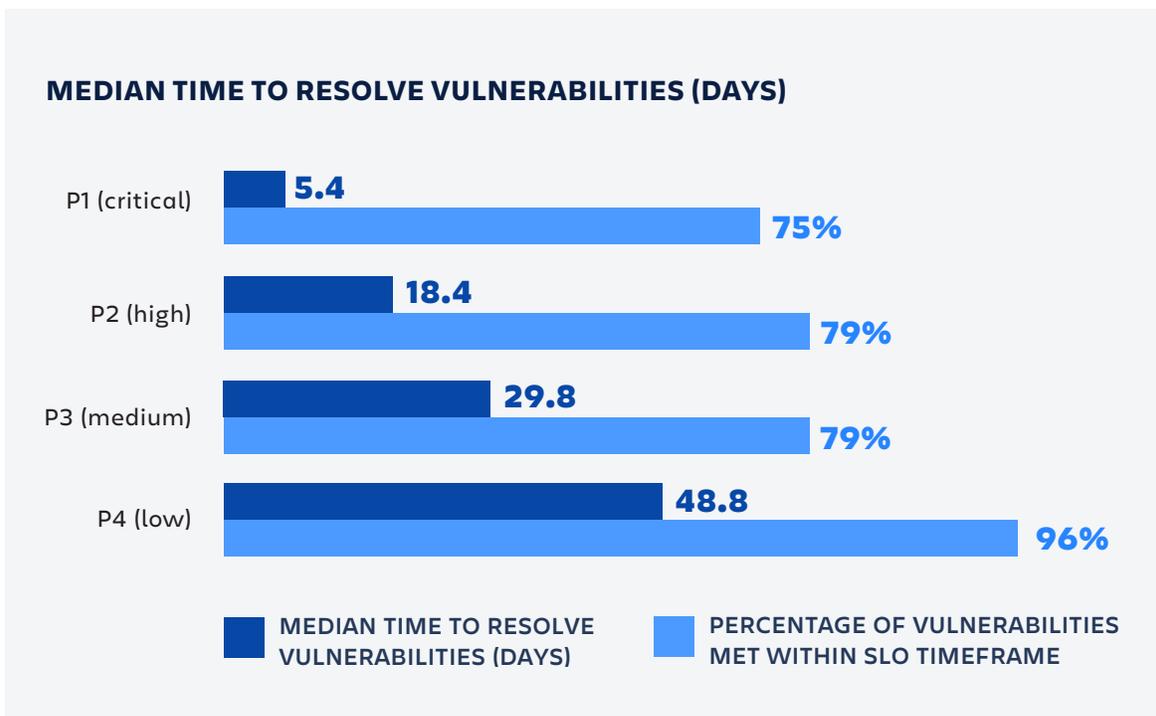
## Bounty payments by vulnerability type

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. 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 security misconfigurations, however the latter category had a higher total payout by almost \$10,000 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.



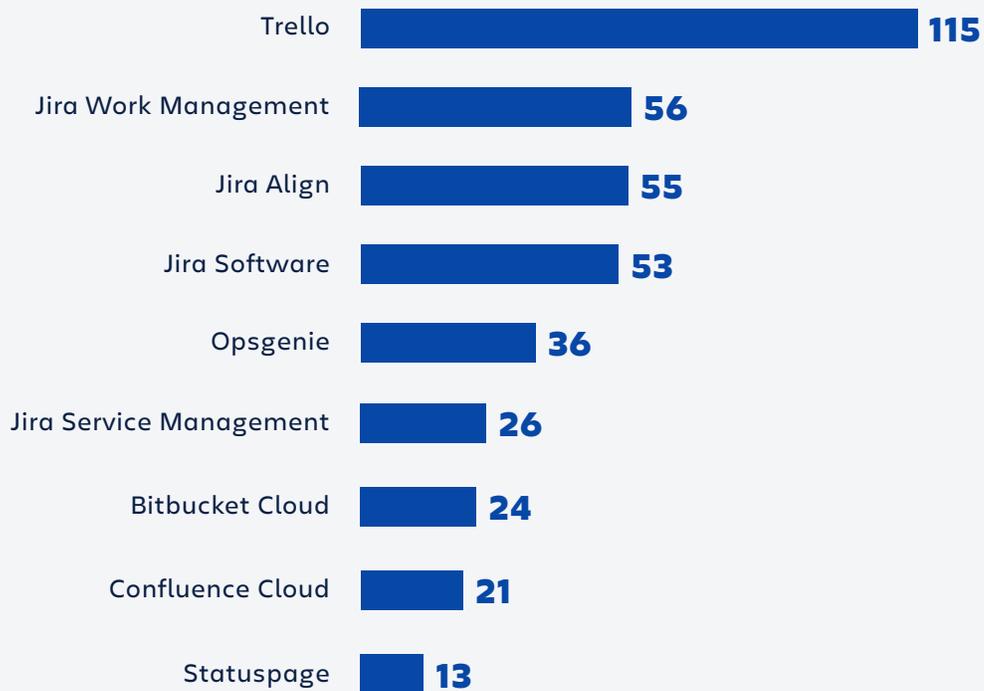
As a point of comparison, Atlassian’s SLOs for different vulnerability types (as per our Security Bug Fix Policy) are listed below:

- 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 FY 21 for which a payment was made. Trello had the largest number of reported vulnerabilities for which payments were made (115), followed by our Jira products (Jira Work Management, Jira Software and Jira Align). Statuspage had the least number, at 13.



## Bounty payments by product

In the below graph, we break down the total bounty payments made by product. Trello had the highest cumulative payout (\$96,800), in addition to having the total highest number of vulnerabilities reported for the financial year.



## 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
theflofly	73
Labda	30
UpdateLap	30
sunilyedla	26
CMSecurity	24
randrly	23
Mr_sharma_	11
Ambrose	9
MrHack	8
AnkitSingh	7
imrannissar	7
al88nsk	7
Hx01	5
Lethal	5
Madhu_Anand	5

## Total payments by researcher

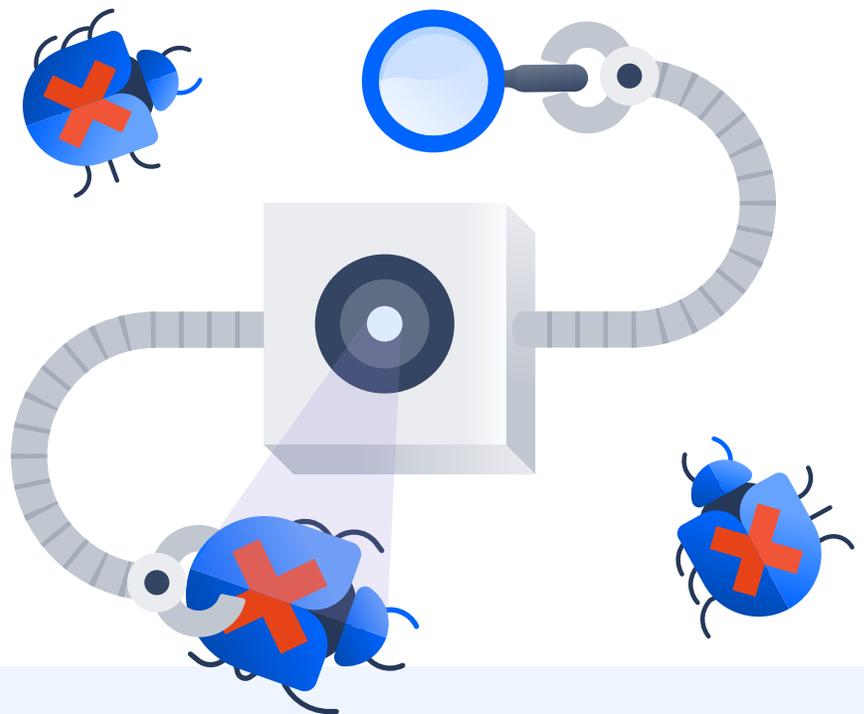
Finally, in the table below we list the top 15 researchers based on total payments received from Atlassian via the bug bounty program during the financial year.

Researcher	Total payout (\$USD)
theflofly	\$54,800
UpdateLap	\$27,650
randrly	\$13,000
Hx01	\$11,400
rjw	\$11,200
Labda	\$9,400
Mr_sharma_	\$8,600
CMSecurity	\$8,400
ajxchapman	\$8,000
imrannissar	\$7,800
MrHack	\$7,800
p3rr0	\$7,200
sunilyedla	\$6,400
Ambrose	\$5,900
AnkitSingh	\$5,700

## 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](#).