PROJECT CleanBeach

Monthly Report

FOSS Risk Assessment
June 2024

OpenRefactory publishes this monthly report to assist developers using **Open Source components** to get the most up to date information on newly discovered security and reliability vulnerabilities.

OPENREFACTORY | Santa Clara, CA

Summary Rollup

This section provides the summary results of the current month's analysis along with the 6-month trends.

Bugs Reported and Fixed in June – At a Glance

A total of 1,198 projects were scanned in June with all of the projects being part of the continuing effort to analyze the PyPI projects. There was one new bug filed. A check of past analysis was done revealing 2 past bugs which have been reclassified. The newly discovered issue was a Security/Reliability bug of Medium Severity. One of the 2 reclassified bugs was also a Security/Reliability bug of Medium Severity with the other being Low Severity. Here is the summary breakdown:

Bugs Reported

Total bugs filed	1
Security/Reliability bugs filed	2 (1 bug reclassified from an earlier analysis)
High Severity Bugs	0
Bugs with a fix suggestion	0

Bugs Fixed

Fixes merged by maintainers	1
Fixes ignored by maintainers	2

In June one fix from past analyses was merged by the maintainers. However, there were 2 fixes that were ignored by the maintainers.

Projects in Which a Bug Was Reported

These are the projects which were found to contain the issues reported in the previous section. The name of the project and related version number is provided along with the title of the bug.

There is a link associated with that title so that bug context can be found by clicking on the link.

In June 1 new bug was filed and 2 bugs were reclassified. They are also shown here.

Project Name	Language	Version	Severity	Bug Category & Link	Resolution
Jenkins	Java	2.461	Medium	Null Dereference	Merged
Jenkins	Java	2.461	Low	Missing "serialVersionUID" in Serializable Class	Merged
Jenkins	Java	2.461	Medium	Null Dereference	Merged

Cumulative Results
(6-month rolling window)

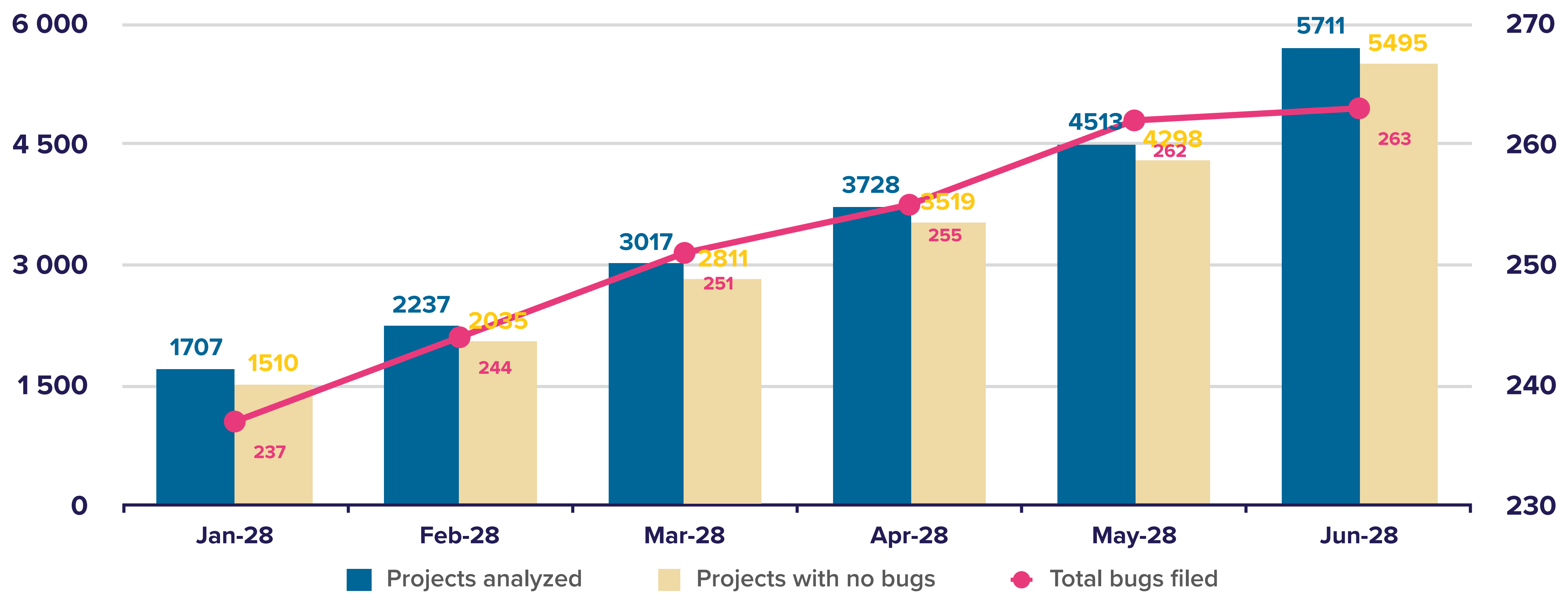
This section provides a rolling view of the progress being made in cleaning up the Open Source project libraries.

Project analysis progress

The graph below provides a view on the long-term progress of tackling the security of the Open Source libraries. It shows a 6-month window with the last month being the current month. To date, 5,711 projects have been scanned with 5,495 having no issues uncovered.

There have been 263 projects scanned with bug reports filed.

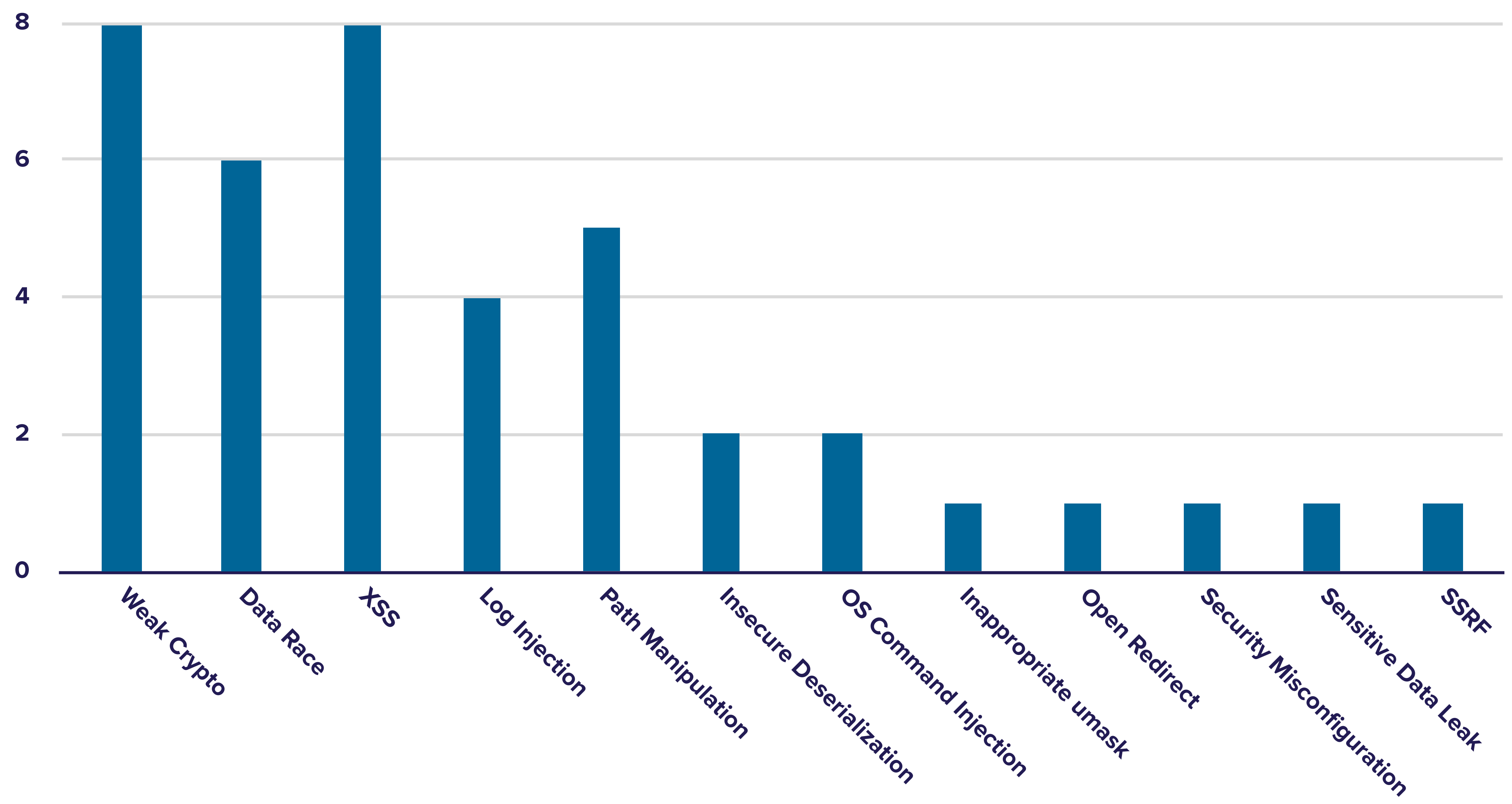
Cumulative Analysis Progress



High Severity Bug Distribution for the Last 6 Months

This section focuses upon the subset of total bugs which are High Severity. It shows how those important bugs are distributed across the various bug classes. To date, a total of **40 High-Severity issues** have been detected and reported.

Cumulative High Severity Bugs Detected



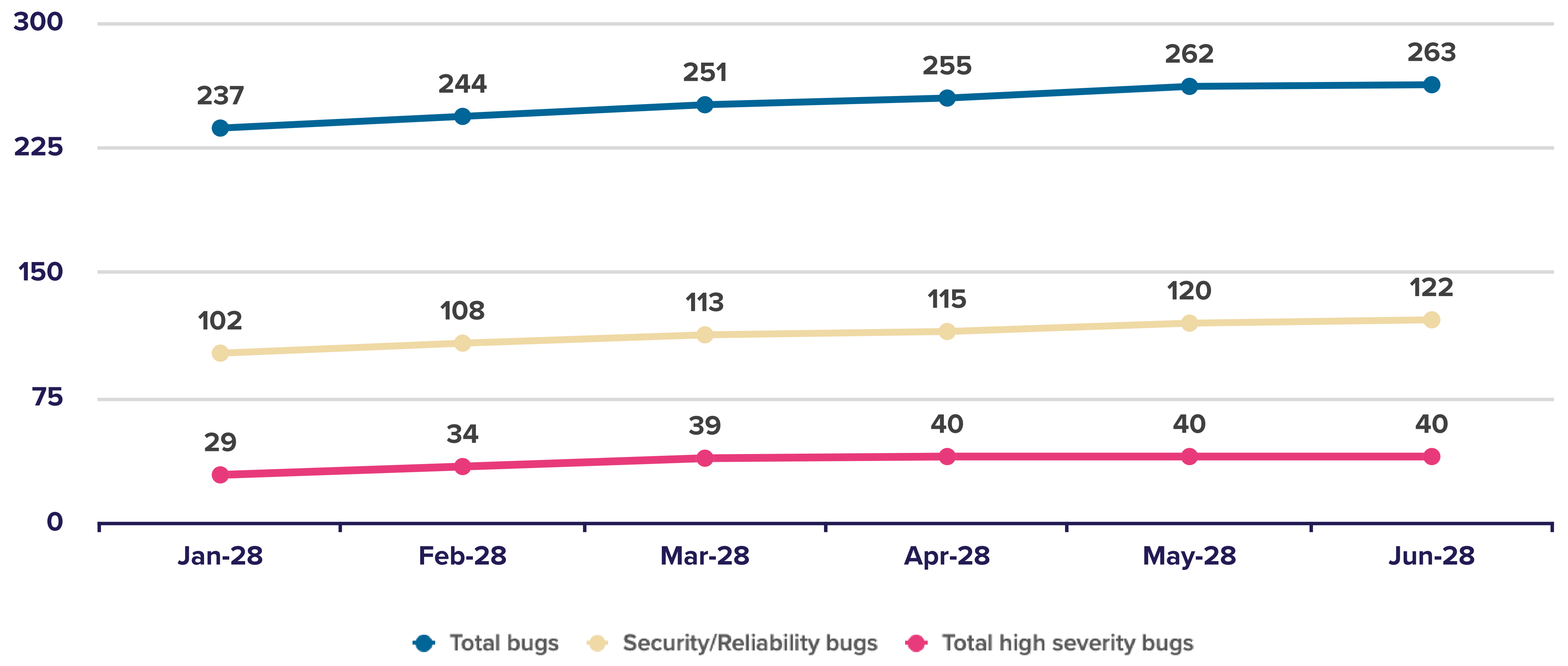
Total Bug Distribution for the Last 6 Months

This section broadens the view of the cumulative analyses by showing the status across all of the bugs uncovered over the last 6-months.

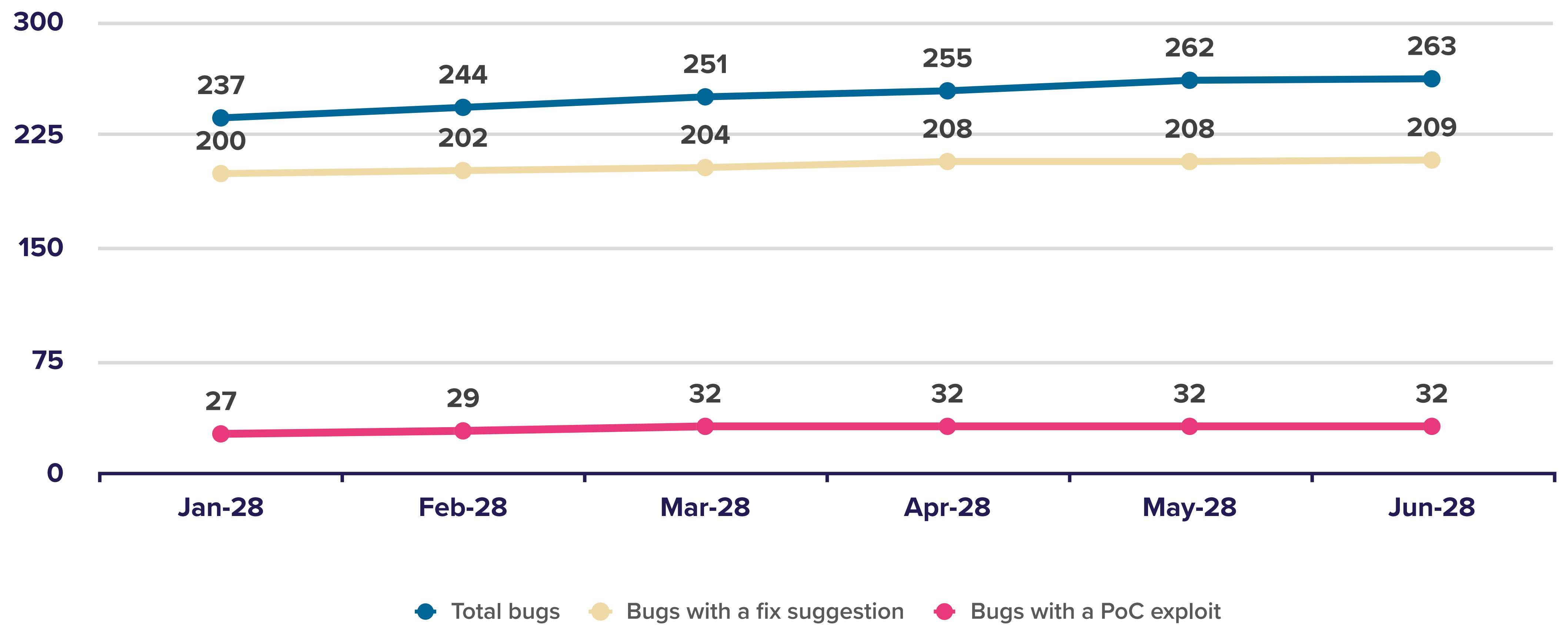
From here, it can be seen how the bug mediation process is proceeding. Pie charts are used to show the proportions.

	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24
Total bugs filed	237	244	251	255	262	263
Security/Reliability bugs filed	102	108	113	115	120	122
Total high severity bugs filed*	29	34	39	40	40	40
Bugs with a fix suggestion	200	202	204	208	208	209
Bugs with a PoC exploit	27	29	32	32	32	32

Bug Detection Trend | *Cumulative bug detection trend as of 06 - 2024*



Trend in Bug Reporting Outcomes | *Cumulative trend showing outcomes from bug reporting as of 06-2024*



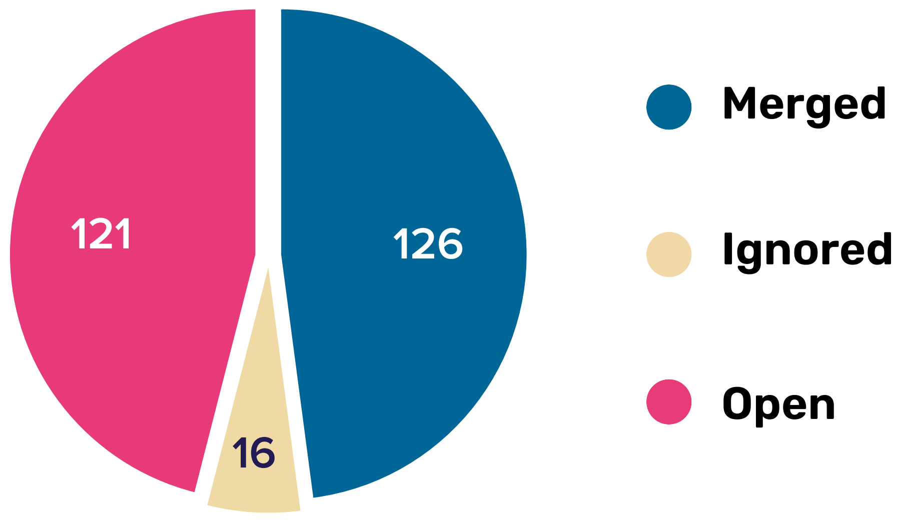
Fix Progress for the Last 6 Months

This section demonstrates the response from the maintainer community in terms of recognizing and addressing the issues that have been reported.

The trend shows that most maintainers are not ignoring the reported issues and address them over time.

	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24
Fixes merged by maintainers	113	118	121	125	125	126
Security/Reliability fixes merged	37	39	40	40	40	40
Fixes ignored by maintainers	11	12	12	14	14	16
Reports still open	113	114	118	116	123	121

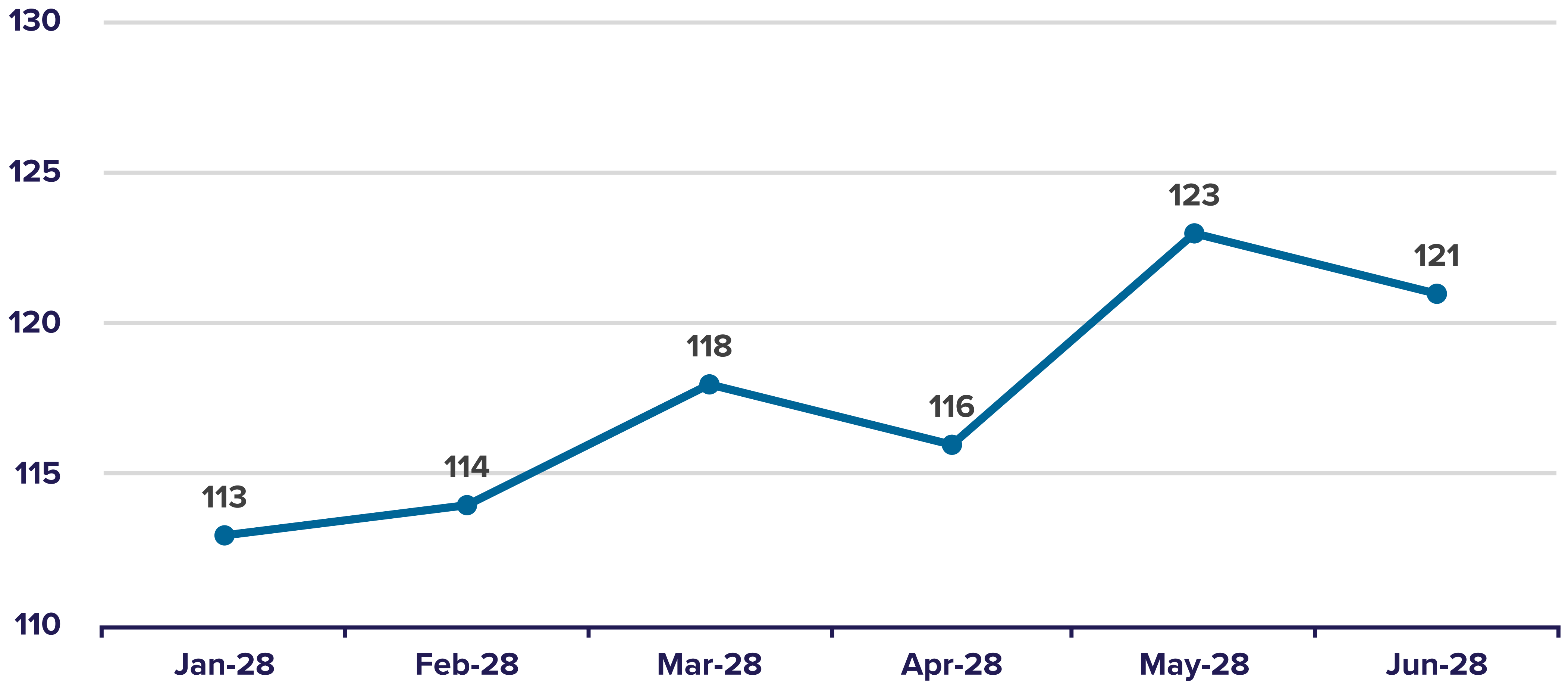
Bug fixing activity as of June 2024



Reports Still Open

The chart below shows the trend for reports that remain open. Open reports are bugs that have been filed with the maintainers but not yet addressed. In general, this trend should be roughly the same as the overall trend in new bug detection.

A downward trend implies maintainers are doing well to stay on top of their security notices. An upward trend may indicate that maintainers are taking longer than desirable to clear out their security issues.



Get in touch **with us**

pcb-info@openrefactory.com