PROJECT CleanBeach

Monthly Report

FOSS Risk Assessment
August 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 August – At a Glance

A total of 1,206 projects were scanned in August with all of the projects being part of the continuing effort to analyze the PyPI projects.

There were no new bugs detected but updates occurred due to recategorization of an older previously filed bug and the removal of a duplicate filed bug.

The net result is a reduction in the total number of filed bugs but an addition to the number of High Severity Bugs as 2 bugs filed earlier had their severities updated and another Medium Severity bug was upgraded.

Bugs Reported

Total bugs filed	-1 (Removed a duplicate bug from earlier)
Security/Reliability bugs filed	1
High Severity Bugs	2
Bugs with a fix suggestion	19

Bugs Fixed

Fixes merged by maintainers	7
Fixes ignored by maintainers	6

In August, a number of previous filed bugs were updated with Fix suggestions. The maintainers for 7 bugs responded and merged in their fixes. However, 6 bugs were dismissed 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.

Project Name	Language	Version	Severity	Bug Category & Link	Resolution
ckan	Python	2.9.9	High	Weak Crypto	Accepted
python-microscopy	Python	3e6e5f24b0920f892b...	High	Log Injection	Open
core-java-spring	Java	4.6.1	Medium	Missing "serialVersionUID" in Class	Accepted

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

These 3 bugs represent 2 older bugs that were determined to have been incorrectly classified and are now updated to be High Severity. Also, another older bug was upgraded from a Low Severity "Logical" bug to Medium Severity.

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.

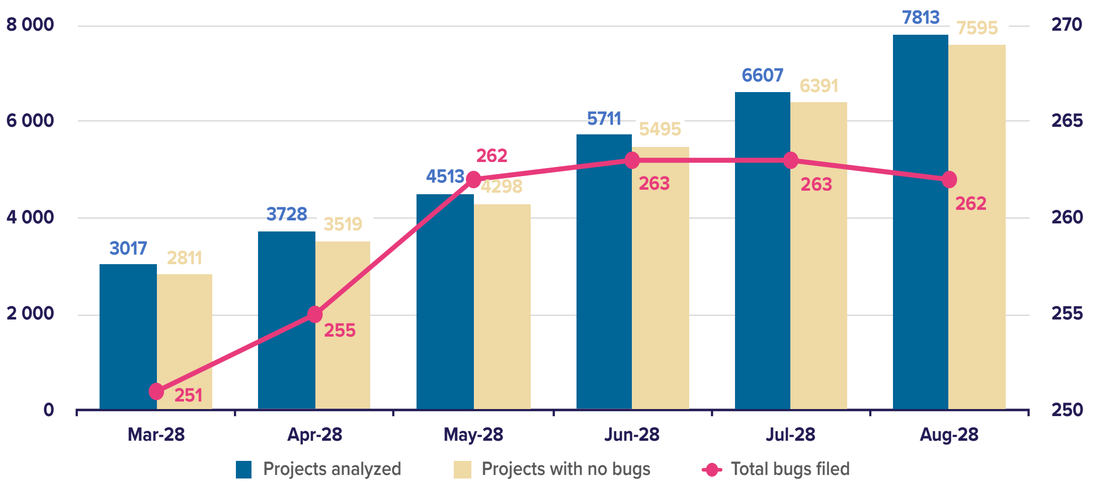
Project analysis progress

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, 7,813 projects have been scanned with 7,595 having no issues uncovered.

There have been 262 projects scanned with bug reports filed.

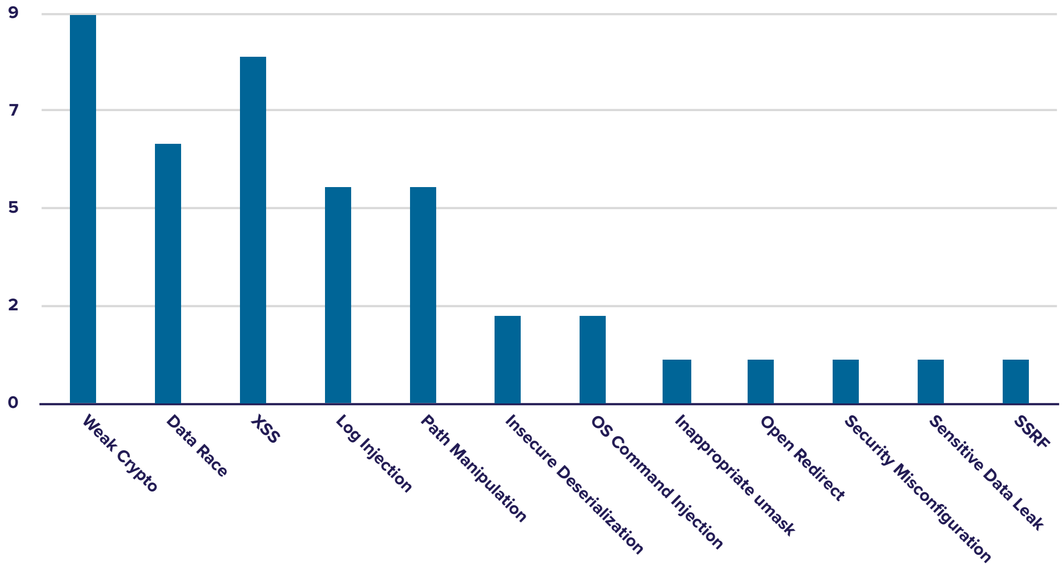
Cumulative Analysis Progress



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 **42 High-Severity issues** have been detected and reported.

Cumulative High Severity Bugs Detected



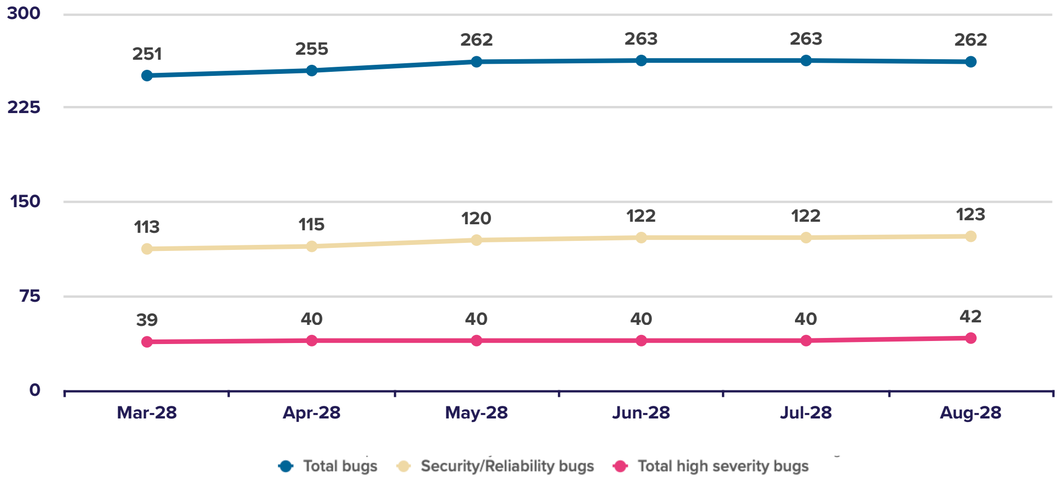
Total Bug Distribution for the Last 6 Months

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

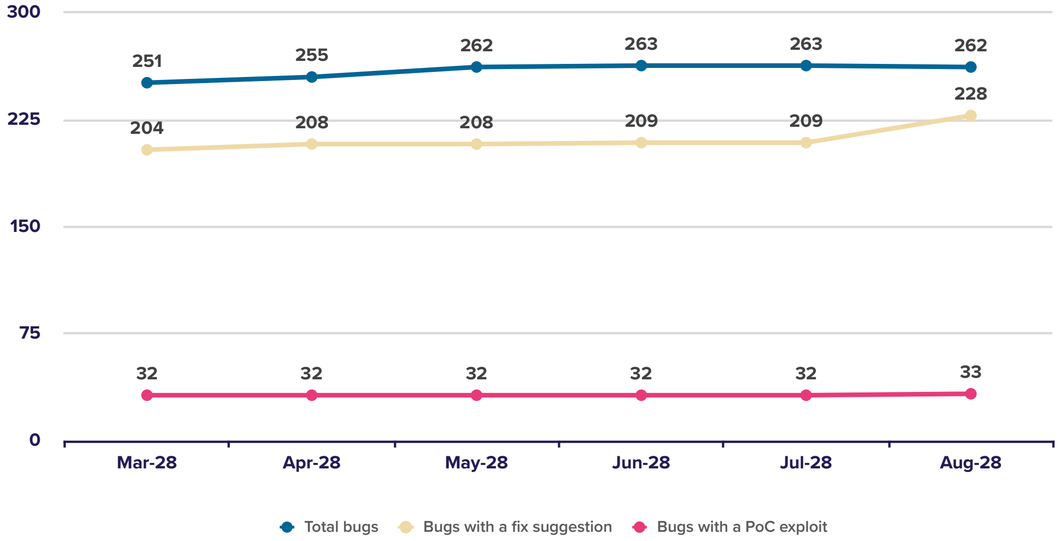
From here, it can be seen how the bug mediation process is proceeding. Pie charts are used to show the proportions.

	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24
Total bugs filed	251	255	262	263	263	262
Security/Reliability bugs filed	113	115	120	122	122	123
Total high severity bugs filed*	39	40	40	40	40	42
Bugs with a fix suggestion	204	208	208	209	209	228
Bugs with a PoC exploit	32	32	32	32	32	33

Bug Detection Trend | *Cumulative bug detection trend as of 08 - 2024*



Trend in Bug Reporting Outcomes | *Cumulative trend showing outcomes from bug reporting as of 08-2024*



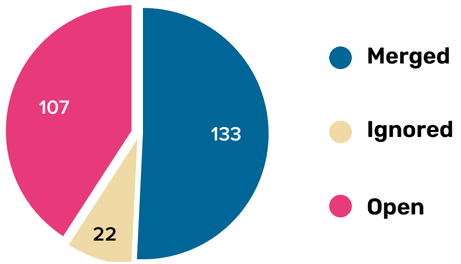
Fix Progress for the Last 6 Months

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.

	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24
Fixes merged by maintainers	121	125	125	126	127	133
Security/Reliability fixes merged	40	40	40	40	41	48
Fixes ignored by maintainers	12	14	14	16	16	22
Reports still open	118	116	123	121	120	107

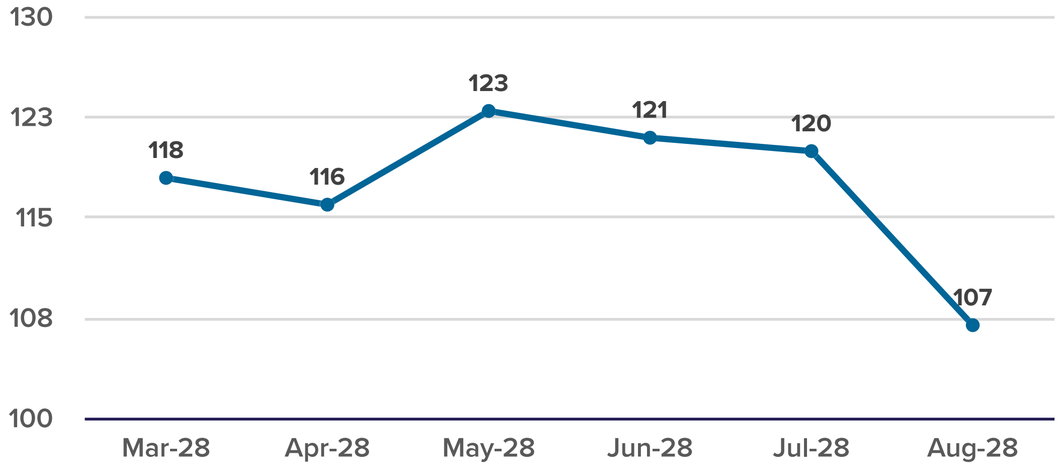
Bug fixing activity as of August 2024



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