PROJECT CleanBeach

MONTHLY REPORT

FOSS Risk Assessment
November 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 November – At a Glance

A total of 597 projects were scanned in November with an emphasis on the PyPI libraries with 535 artifacts being analyzed.

Additionally, 56 Go projects, which are part of the Kubernetes project, were analyzed.

Finally, a few more Java projects, 6 of them, related to Jenkins were analyzed.

Bugs Reported	
Total bugs filed	3
Security/Reliability bugs filed	3
High Severity Bugs	2
Bugs with a fix suggestion	3

Bugs Fixed	
Fixes merged by maintainers	2
Fixes ignored by maintainers	0

In November. the team focused on analysis of the Kubernetes project, written in Go as a continuing effort with Alpha Omega to be of benefit to specific projects. When that was completed, the effort focused again on the PyPI libraries and the completion of the Jenkins analysis begun last month.

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.

These 3 bugs bugs filed with 2 of them being the result of the Go analyses and one being found in Java as part of the Jenkins effort. No new bugs were filed in the PyPI analyses.

Project Name	Language	Version	Severity	Bug Category & Link	Resolution
cadence	Go	1.12.13	High	Deadlock	Accepted
bc-java	Java	1.78.1	Medium	Null Dereference	Open
google-cloud-go	Go	1.69.0	High	Channel Blocking	Accepted

Cumulative Results (6-month rolling window)

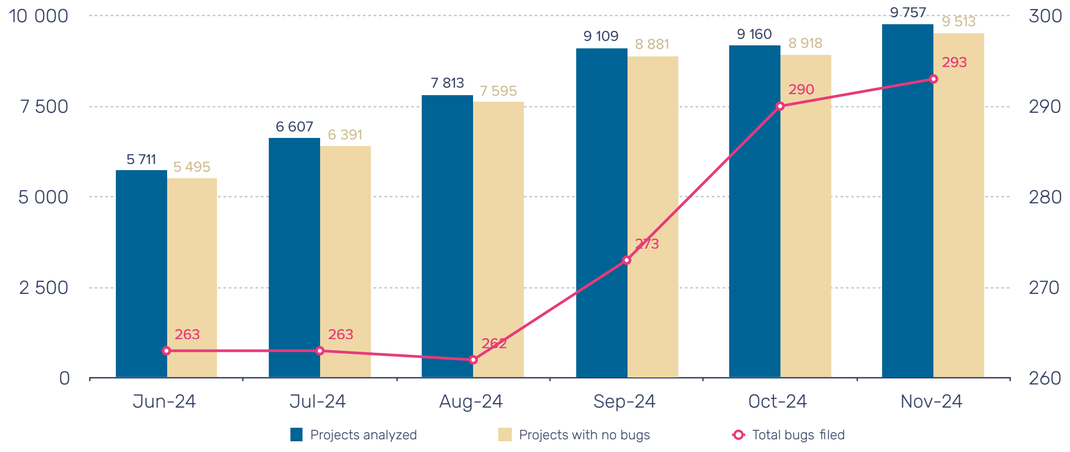
This section provides a rolling view of the progress being made in cleaning up the Open Source project libraries.

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, 9,109projects have been scanned with 8,881 having no issues uncovered.

There have been 273 projects scanned with bug reports filed.

Cumulative Analysis Progress

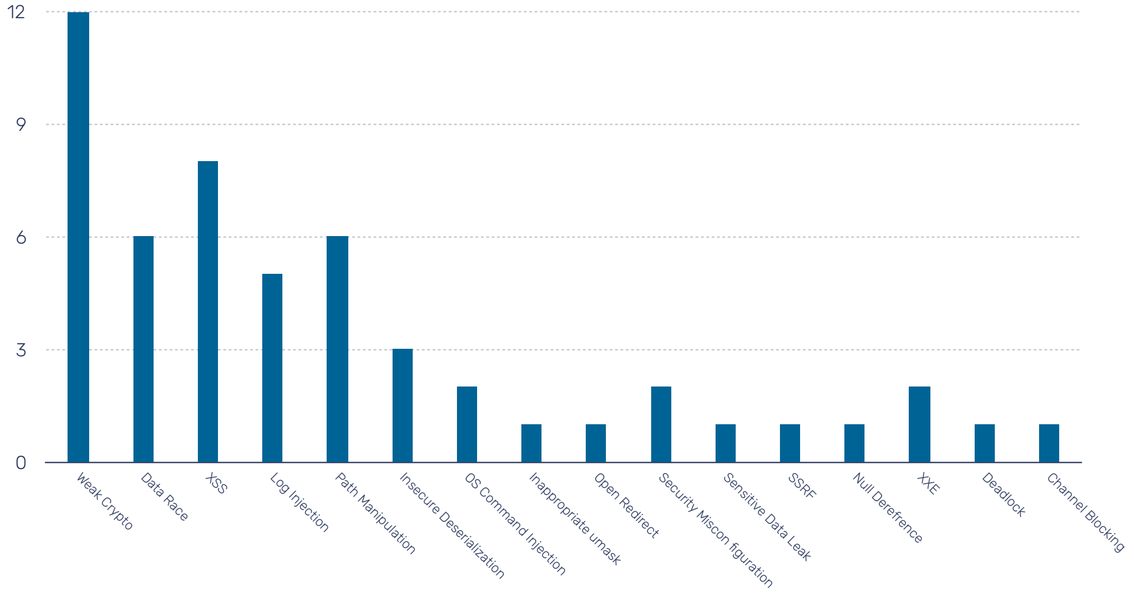


High Severity Bug Distribution for the Last 6 Months

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.

Cumulative High Severity Bugs Detected

To date, a total of 53 High-Severity issues have been detected and reported.

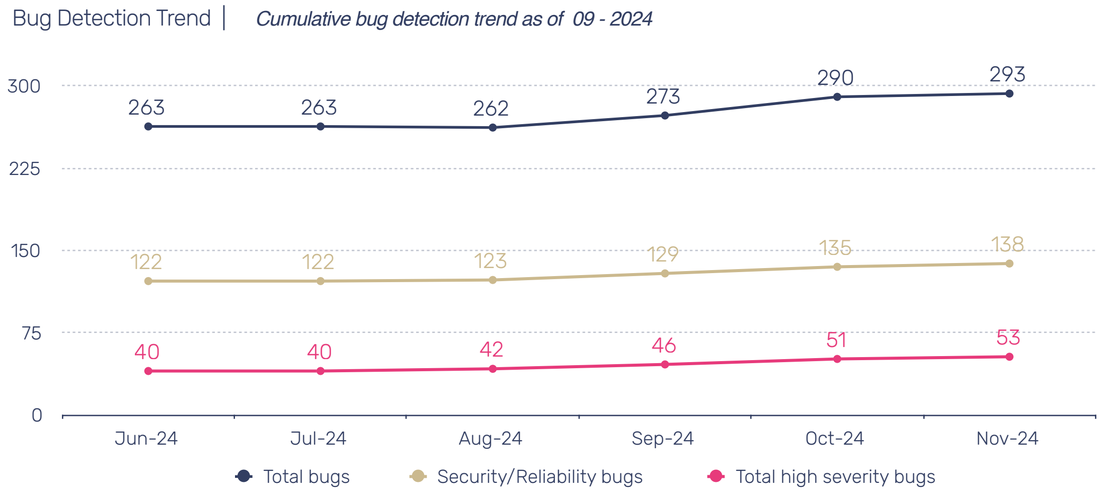


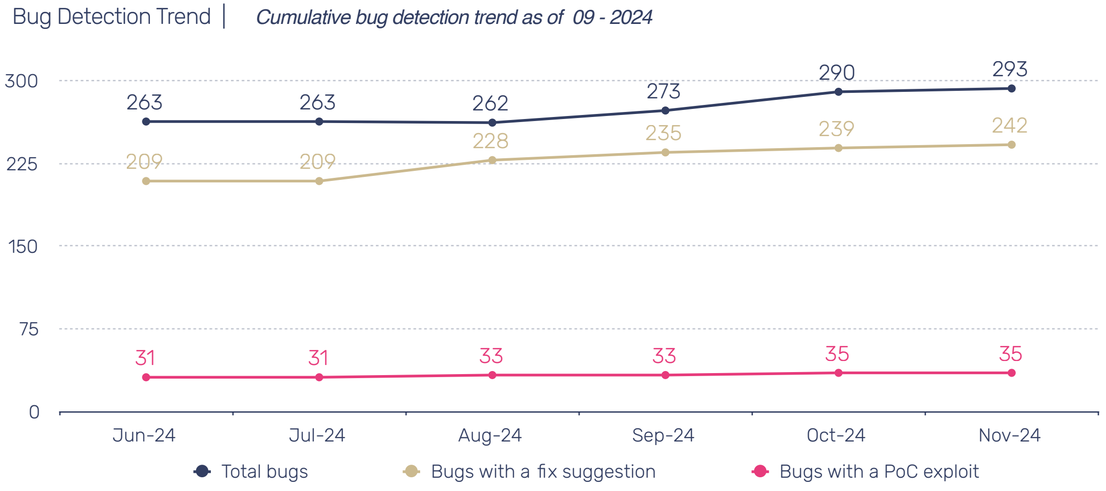
Total Bug Distribution for the Last 6 Months

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

	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24
Total bugs filed	263	263	262	273	290	293
Security/Reliability bugs filed	122	122	123	129	135	138
Total high severity bugs filed*	40	40	42	46	51	4536
Bugs with a fix suggestion	209	209	228	235	239	232425
Bugs with a PoC exploit	32	32	33	33	35	35

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





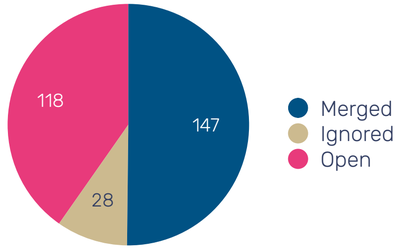
Fix Progress for the Last 6 Months

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.

	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24
Fixes merged by maintainers	126	127	133	140	145	147
Security/Reliability fixes merged	40	41	48	49	52	54
Fixes ignored by maintainers	16	16	22	22	28	28
Reports still open	121	120	107	111	117	118

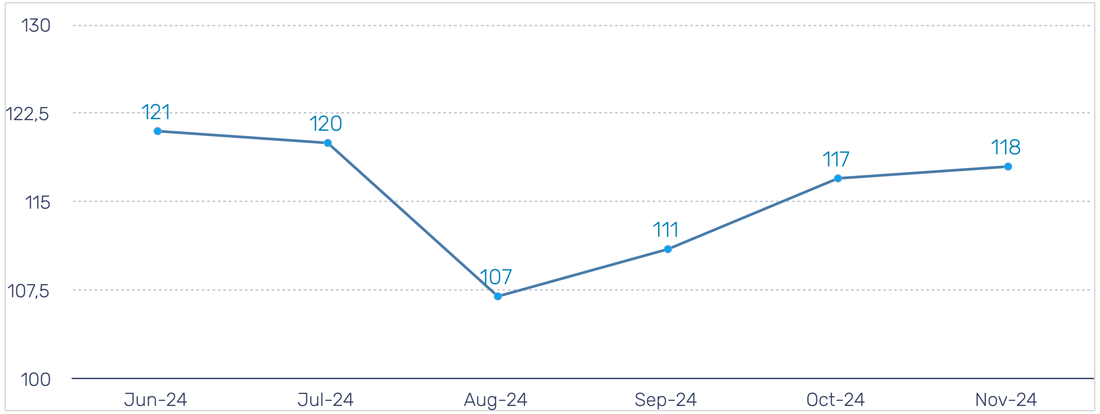
Bug fixing activity as of November 2024



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