CURL AND LIBCURL

THE END OF THE CURL BUG-BOUNTY

JANUARY 26, 2026 | DANIEL STENBERG | 2 COMMENTS

tldr: an attempt to reduce the *terror reporting*.

There is no longer a curl bug-bounty program. It officially stops on January 31, 2026.

After having had a few half-baked previous takes, in April 2019 we kicked off the first real curl bug-bounty with the help of Hackerone, and while it stumbled a bit at first it has been quite successful I think.

We attracted skilled researchers who reported plenty of actual vulnerabilities for which we paid fine monetary rewards. We have certainly made curl better as a direct result of this: **87 confirmed vulnerabilities and over 100,000 USD** paid as rewards to researchers. I'm quite happy and proud of this accomplishment.

I would like to especially highlight the awesome Internet Bug Bounty project, which has paid the bounties for us for many years. We could not have done this without them. Also of course Hackerone, who has graciously hosted us and been our partner through these years.

Thanks!

How we got here

Looking back, I think we can say that the downfall of the bug-bounty program started slowly in the second half of 2024 but accelerated badly in 2025.

We saw an explosion in AI slop reports combined with a lower quality even in the reports that were not obvious slop – presumably because they too were actually misled by AI but with that fact just hidden better.

Maybe the first five years made it possible for researchers to find and report the low hanging fruit. Previous years we have had a rate of somewhere north of 15% of the submissions ending up confirmed vulnerabilities. Starting 2025, the confirmed-rate plummeted to below 5%. Not even one in twenty was *real*.

The never-ending slop submissions take a serious mental toll to manage and sometimes also a long time to debunk. Time and energy that is completely wasted while also hampering our will to live.

I have also started to get the feeling that a lot of the security reporters submit reports with a *bad faith attitude*. These "helpers" try too hard to twist whatever they find into something horribly bad and a critical vulnerability, but they rarely actively contribute to actually *improve* curl. They can go to extreme efforts to argue and insist on their specific current finding, but not to write a fix or work with the team on improving curl long-term etc. I don't think we need more of that.

There are these three bad trends combined that makes us take this step: the mind-numbing AI slop, humans doing worse than ever and the apparent will to poke holes rather than to help.

Actions

In an attempt to do something about the sorry state of curl security reports, this is what we do:

- We no longer offer any monetary rewards for security reports – no matter which severity. In an attempt to remove the incentives for submitting made up lies.
- We stop using Hackerone as the recommended channel to report security problems. To make the change immediately obvious and because without a bug-bounty program we don't need it.
- We refer everyone to submit suspected curl security problems on GitHub using their *Private vulnerability reporting* feature.
- We continue to immediately *ban and publicly ridicule* everyone who submits AI slop to the project.

Maintain curl security

We believe that we can maintain and continue to evolve curl security in spite of this change. Maybe even improve thanks to this, as hopefully this step helps prevent more people pouring sand into the machine. Ideally we reduce the amount of wasted time and effort.

I believe the best and our most valued security reporters still will tell us when they find security vulnerabilities.

Instead

If you suspect a security problem in curl going forward, we advise you to head over to GitHub and submit them there.

Alternatively, you send an email with the full report to `security @ curl.se`.

In both cases, the report is received and handled privately by the curl security team. But with *no monetary reward offered*.

Leaving Hackerone

Hackerone was good to us and they have graciously allowed us to run our program on their platform for free for many years. We thank them for that service.

As we now drop the rewards, we feel it makes a clear cut and displays a clearer message to everyone involved by also moving away from Hackerone as a platform for vulnerability reporting. It makes the change more visible.

Future disclosures

It is probably going to be harder for us to publicly disclose every incoming security report in the same way we have done it on Hackerone for the last year. We need to work out something to make sure that we can keep doing it at least imperfectly, because I believe in the goodness of such transparency.

We stay on GitHub

Let me emphasize that this change does not impact our presence and mode of operation with the curl repository and its hosting on GitHub. We hear about projects having problems with low-quality AI slop submissions on GitHub as well, in the form of issues and pull-requests, but for curl we have not (yet) seen this – and frankly I don't think switching to a GitHub alternative saves us from that.

Other projects do better

Compared to others, we seem to be affected by the sloppy security reports to a higher degree than the average Open Source project.

With the help of Hackerone, we got numbers of how the curl bug-bounty has compared with other programs over the last year. It turns out curl's program has seen more volume and noise than other public open source bug bounty programs in the same cohort. Over the past four quarters, curl's inbound report volume has risen sharply, while other bounty-paying open source programs in the cohort, such as Ruby, Node, and Rails, have not seen a meaningful increase and have remained mostly flat or declined slightly. In the chart, the pink line represents curl's report volume, and the gray line reflects the broader cohort.