OpenSSL Foundation

Delivering the Mission

Matt Caswell, Executive Director, OpenSSL Foundation

OpenSSL Conference 2026 · Prague · October 15, 2026

OpenSSL Foundation team

Matt Caswell, Executive Director & Principal Software Engineer

Tomáš Mráz, Chief Technology Officer

Richard Levitte, Distinguished Software Engineer

Sherry S. Handel, Deputy Executive Director

Jon Ericson, OpenSSL Communities Manager

Daniel Kubec, Senior Software Engineer

Igor Ustinov, Senior Software Engineer

Ryan Hooper, Associate OpenSSL Foundation Engineer

Michelle Mooney, Executive Assistant

What we delivered in the last year

Fixed-width BIGNUM

- Issue #6640: a timing side channel, open since July 2018
- A new fixed-size number type, OSSL_FN, built from scratch
- Private-key operations moved onto it: RSA, ECDSA, ECDH, and DH, plus DSA and SM2
- Functionally complete on the feature branch; some final "tweaking" taking place; aiming for OpenSSL 4.2 (April 2027)

Funded by Sovereign Tech Agency

The issue backlog

- More than 600 long-standing issues closed under the Sovereign Tech Agency milestones
- Open issues down by about a quarter in a year: 1,346 to 1,002
- Community members picked up "help wanted" issues, such as GREASE support, requested since 2019

Backlog work funded by Sovereign Tech Agency

A stronger test suite

- Two new frameworks: memory-allocation failure testing, and unit tests that mock system functions (including on Windows)
- 119 test pull requests, 115 merged; 31 bugs found, 30 fixed
- Coverage up where it was weakest: applications 55% → 61%, BIO code 59% → 74%

Funded by the Nominet DNS Fund; delivered by Jakub Zelenka

None of these is a new feature. All of them pay down technical debt.

And two new features

Encrypted Client Hello

- In OpenSSL 4.0
- Hides which website a connection is for
- Implemented by Stephen Farrell (DEfO project)
- Significant review work by OpenSSL Foundation engineers

DTLS 1.3

- In OpenSSL 4.1
- TLS 1.3 security for datagram traffic, such as live video
- Started externally in 2023 by Frederik Wedel-Heinen
- Finished by Ryan Hooper whose time is donated to the Foundation by Cisco

Scholarships again: 15 recipients

Nine countries, four continents. Please say hello.

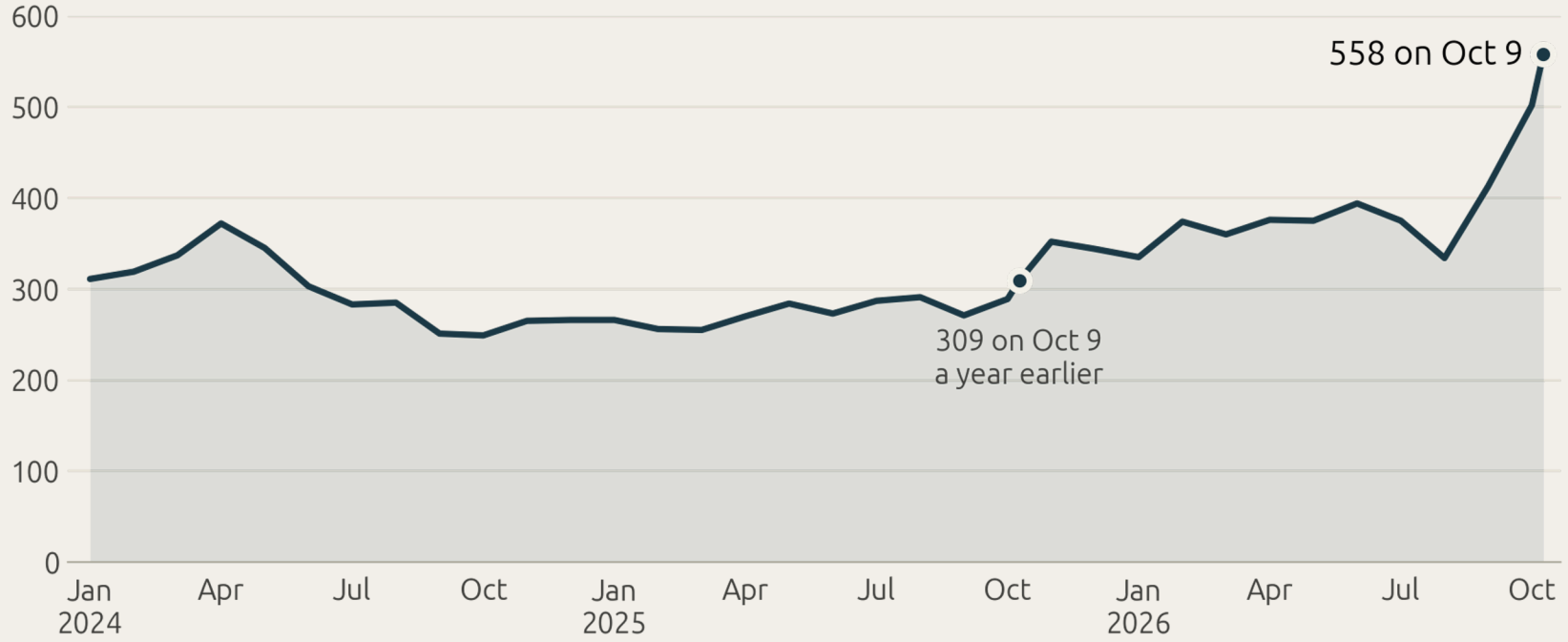
A year in the OpenSSL Library

October 2025	OpenSSL 3.6
April 2026	OpenSSL 4.0: Encrypted Client Hello added; ENGINE and SSLv3 removed
May 2026	New release schedule: a major release every two years (4.2 LTS in April 2027, 5.0 in October 2027)
June 2026	AI policy and updated contributor license agreements
September 2026	OpenSSL 3.0 reaches end of life
October 2026	OpenSSL 4.1, with DTLS 1.3 (due this month)

The work of OpenSSL Foundation, OpenSSL Corporation, and the community

The queue is growing

Open pull requests on openssl/openssl: start of each month from January 2024, and October 9 each year



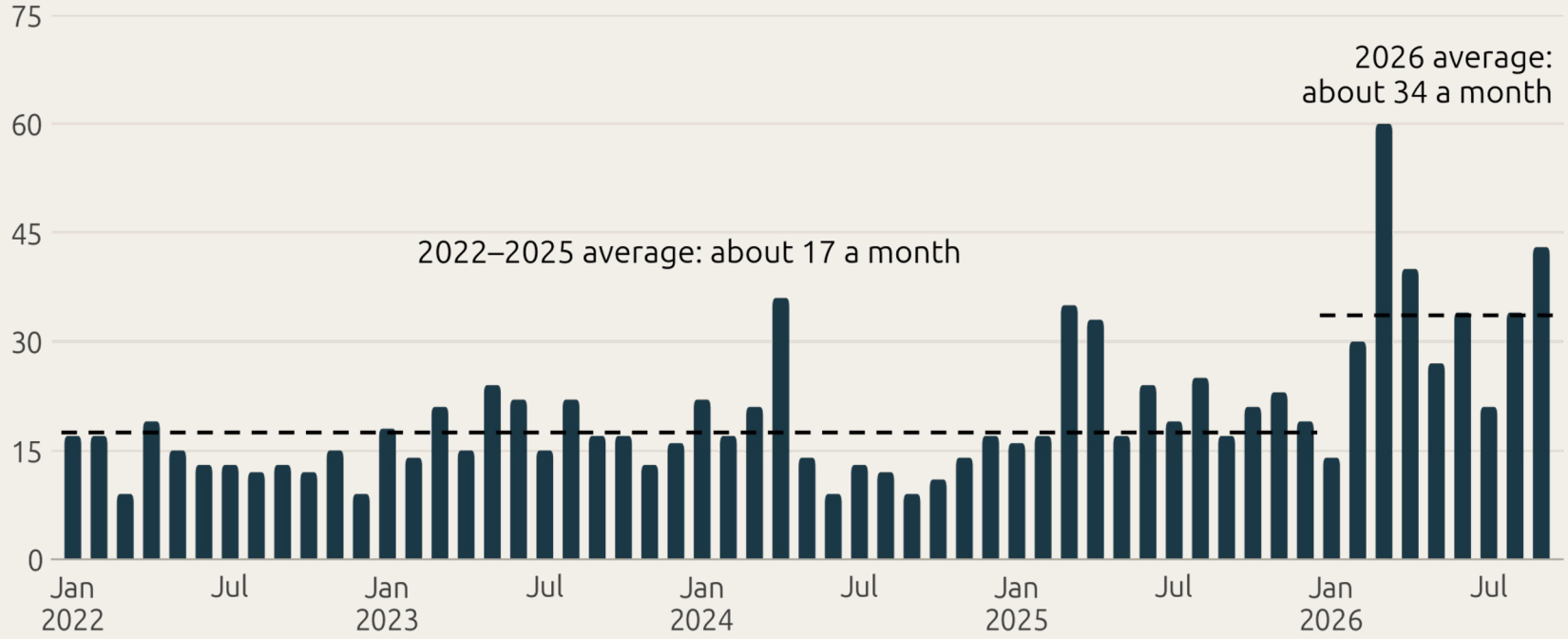
More work landed, but not enough

Jan–Sep	2025	2026	Change
Pull requests opened	1,338	2,604	+95%
Pull requests merged	912	1,541	+69%
Reviews recorded	8,509	13,333	+57%

Pull requests: GitHub, by date opened. Reviews: status.openssl.org, by date written.

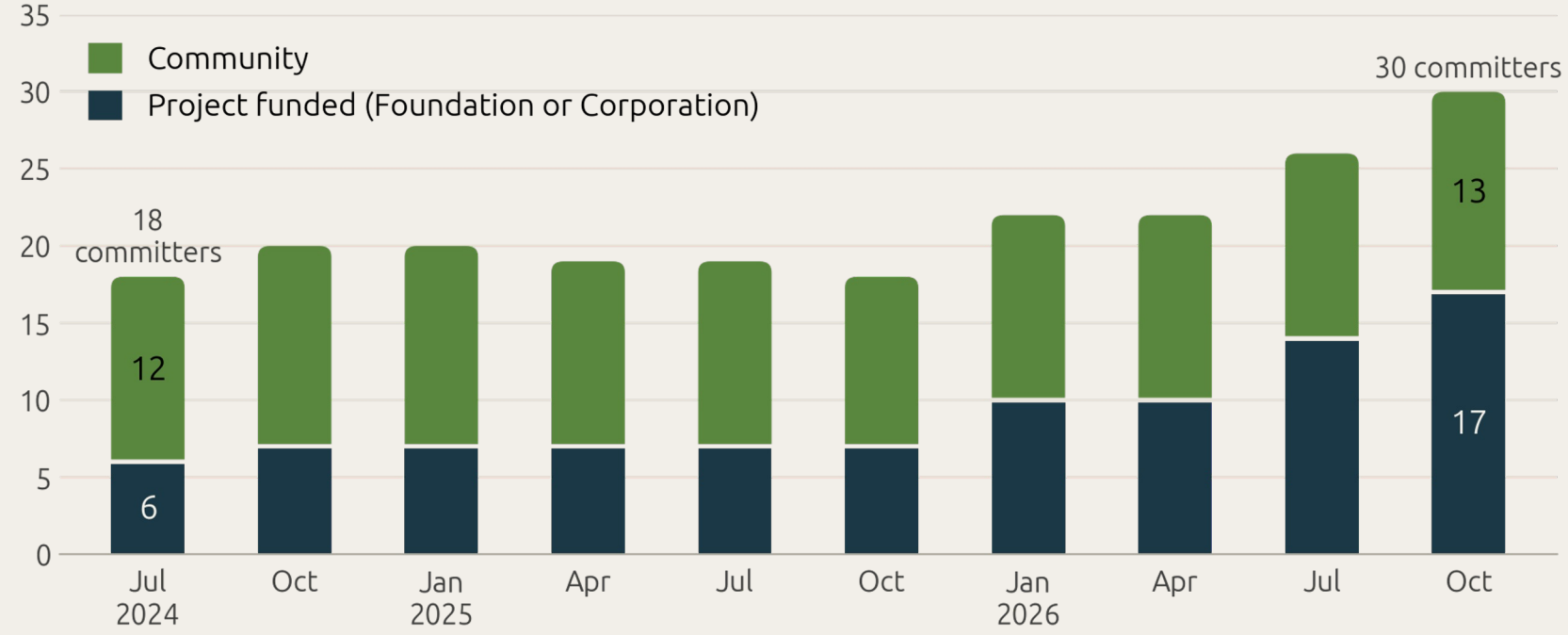
Twice as many new contributors

New external contributors per month: people opening a pull request with nothing previously merged



Who can approve a pull request

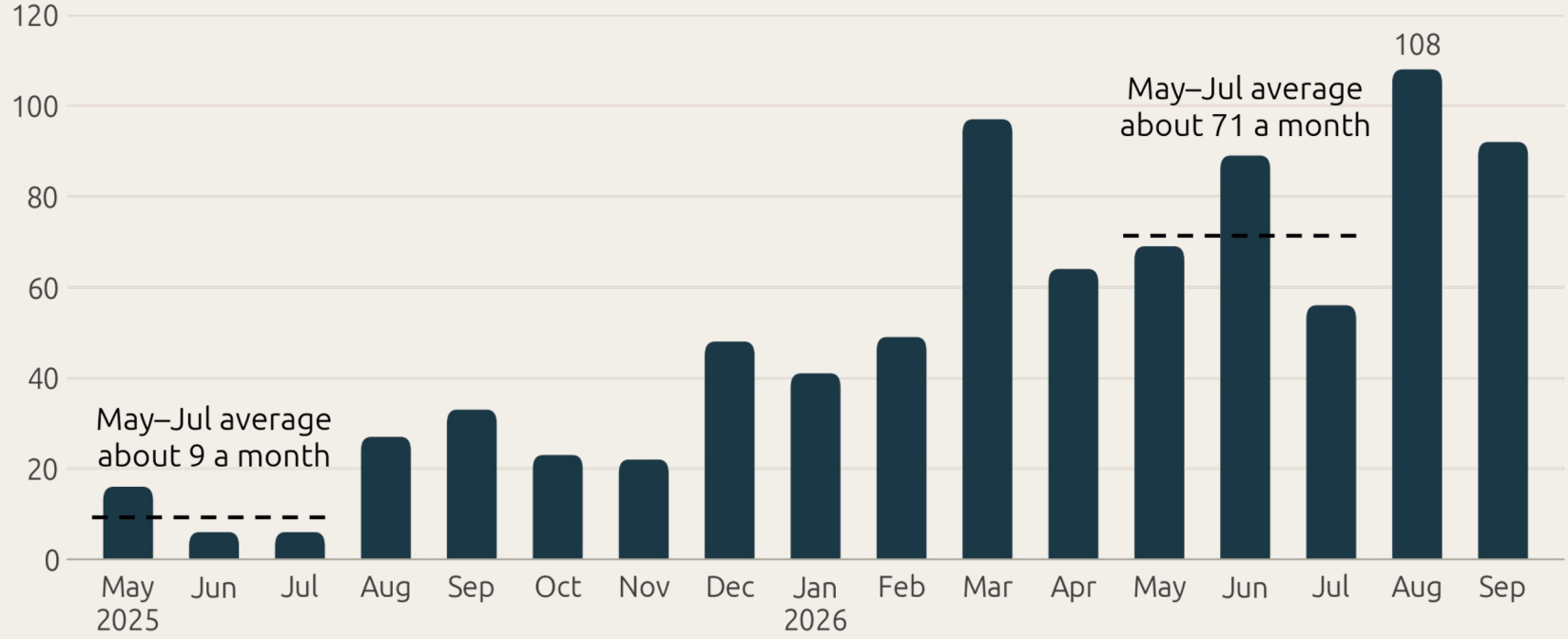
OpenSSL committers at the start of each quarter, July 2024 to October 2026



Security reports: cheap to write, expensive to assess

Reports to the security team

Separate reports and enquiries to OpenSSL's security address each month, May 2025 to September 2026



“AI can increase the speed at which potential problems are discovered. It does not automatically increase the number of experienced engineers available to deal with them.”

Have your say

- One Foundation Advisory Committee now replaces two
- Elected in September; three seats are still vacant: Small Businesses (two) and Committers (one)
- Meet the committee at its panel at this conference
- Join the discussion at openssl-communities.org

What's next

- OpenSSL 4.1, this month, with DTLS 1.3
- OpenSSL 4.2 LTS, April 2027, aiming to include fixed-width BIGNUM
- OpenSSL 5.0, October 2027

How you can help

- Review a pull request in an area you know
- Give your engineers time to review, not only to submit
- Read CONTRIBUTING.md before sending a batch of changes
- Test the pre-releases
- Stand for a vacant advisory committee seat

Critical open source is infrastructure, and needs funding as infrastructure.

Thank you to our leading supporters!

PREMIER SUPPORTERS

Sovereign Tech
Fund

CODE PROTECTORS

craig newmark philanthropies

openSSL Foundation

Data privacy. Secure connections. For everyone.

Thank you

matt@openssl.foundation
openssl.foundation