OpenSSL CONFERENCE

https://openssl-communities.org

The State of the OpenSSL Community

Jon Ericson | Chris Ward

OpenSSL Foundation



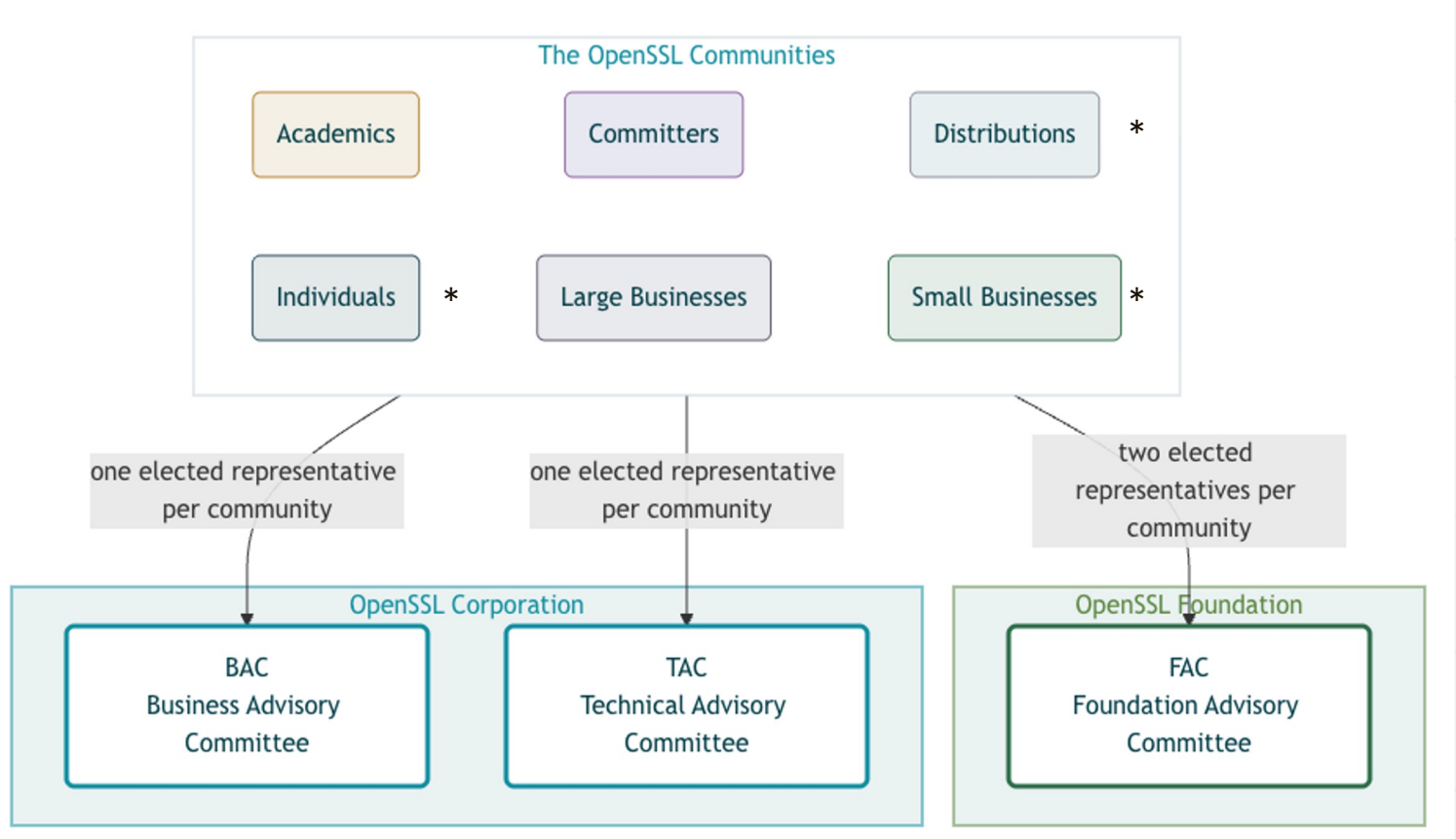


OpenSSL CORPORATION

The OpenSSL Communities



Community Governance



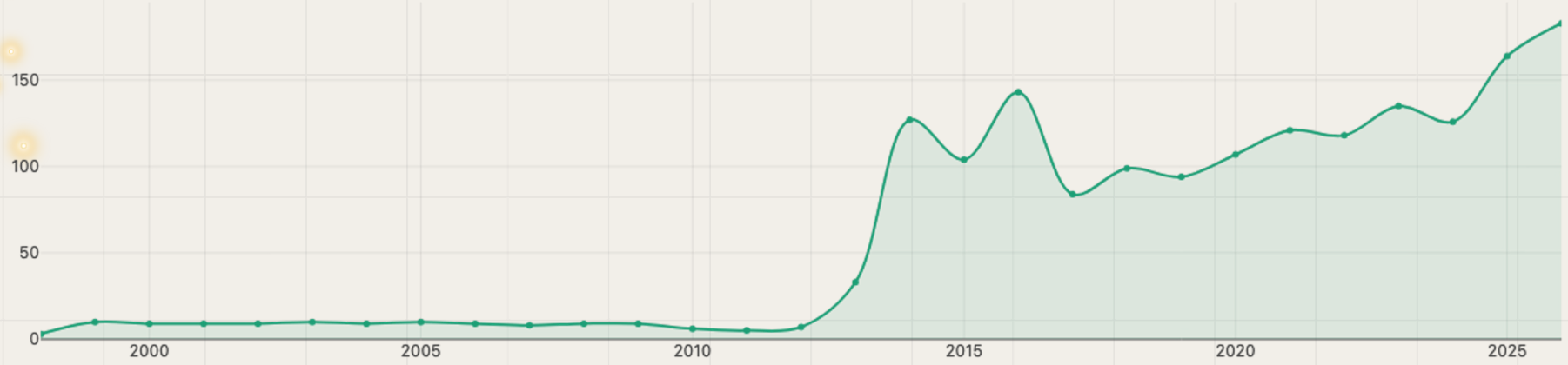
Advisory committees

OpenSSL Corporation: 💼 Business Advisory (BAC), 🛠️ Technical Advisory (TAC)

OpenSSL Foundation: 🏔️ Foundation Advisory Committee (FAC)

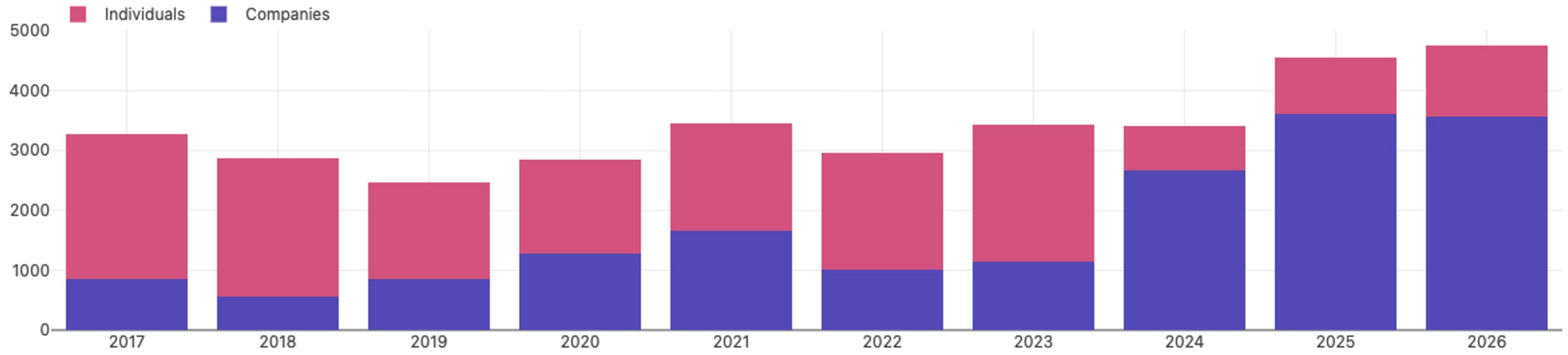


Community Involvement



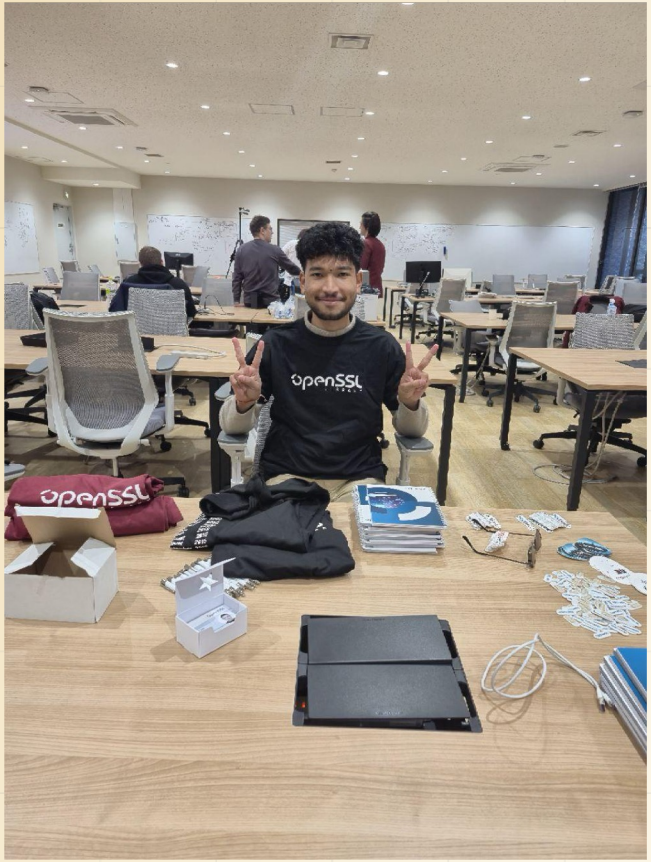
Contributors

Company commits	Individual commits	Company contributors	Individual contributors
51%	49%	41%	59%
avg 2017–present	avg 2017–present	avg 2017–present	avg 2017–present



Individuals





GREASE

Implement RFC 8701 GREASE for TLS ClientHello #30303

Closed mcrmck wants to merge 7 commits into `openssl:master` from `mcrmck:rfc8701-grease`

Conversation 20 | Commits 7 | Checks 94 | Files changed 13 | +451 -3



mcrmck commented on Mar 7 — Contributor

Summary

Implements client-side RFC 8701 GREASE (Generate Random Extensions And Sustain Extensibility) for OpenSSL, addressing #9660 which has been open since 2019.

This picks up where #14560 left off, incorporating the review feedback from **@davidben** and **@paulidale** on that PR:

Reviewers

 t8m ✓

 mattcaswell ✓

Assignees

No one—assign yourself

Labels

approval: ready to merge

Committers

OpenSSL / Committers

31 committers
github.com/orgs/openssl/teams/committers


Alicja Kario
@tomato42


Andrew Dinh
@andrewkdinh


Bernd Edlinger
@bernd-edlinger


Bob Beck
@bob-beck


Daniel Kubec
@n13l


David von Oheimb
@DDvO


Dmitry Belyavskiy
@beldmit


Dmitry Misharov
@quarckster


esyr
@esyr


fwh-dc
@fwh-dc


Igor Ustinov
@igus68


Jakub Zelenka
@bukka


Kurt Roeckx
@kroeckx


Matt Caswell
@mattcaswell


Milan Broz
@mbroz


Mounir IDRASSI
@idrassi


Neil Horman
@nhorman


Nikola Pajkovsky
@npajkovsky


Paul Yang
@InfoHunter


Pauli
@paulidale


Pocs Norbert
@jogme


Richard Levitte
@levitte


Ryan Hooper
@rsith71


Sashan
@Sashan


Shane
@slontis


Simo Sorce
@simo5


Tim Hudson
@t-j-h


Todd Short
@tmshort


Tom Cosgrove
@tom-cosgrove-arm


Tomáš Mráz
@t8m

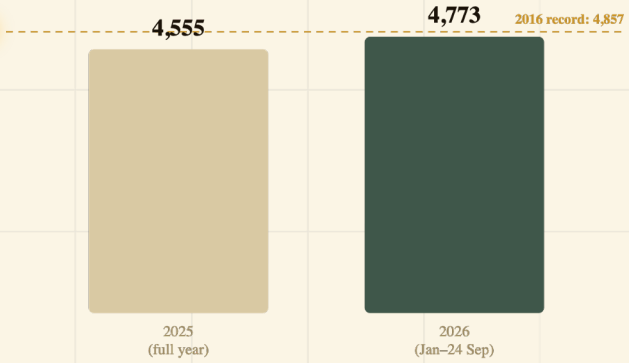

Viktor Dukhovni
@vdukhovni

Source: GitHub org team “committers”, pages 1–2

Generated 2026-09-23

ZOOM IN

Since our last conference in Prague



The first OpenSSL Conference met in Prague October 2025. 2026 has already out-committed all of 2025 — with three months still to go.

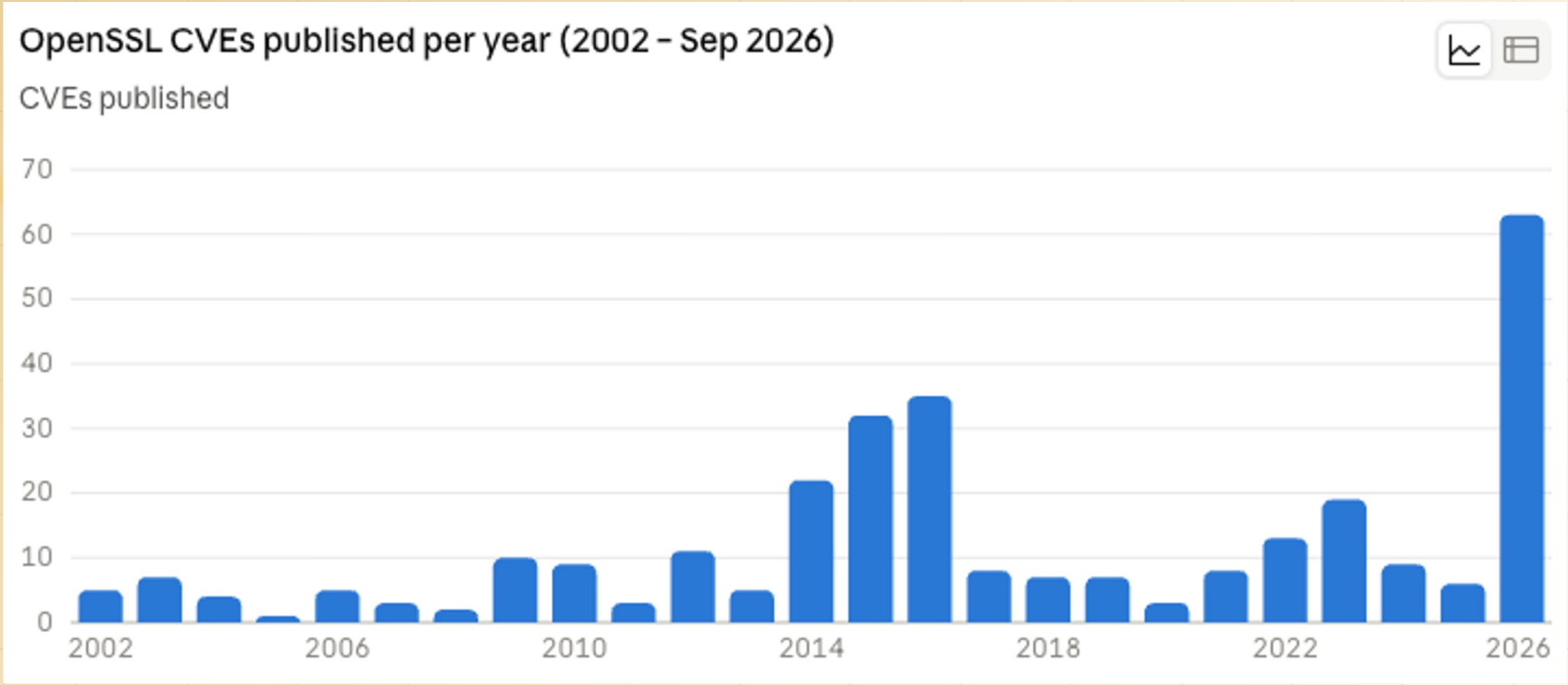
What's kept the pace up

Post-quantum migration work (ML-KEM, ML-DSA), a new DTLS 1.3 implementation, and AVX-512/VAES performance tuning heading into the 4.1 release — the topics on stage in Prague are the ones showing up in the commit log.

SINCE PRAGUE

§ Source: OpenSSL Development Metrics, By Year · conference: openssl-conference.org

Automated vulnerability reporting has arrived



New AI Policy

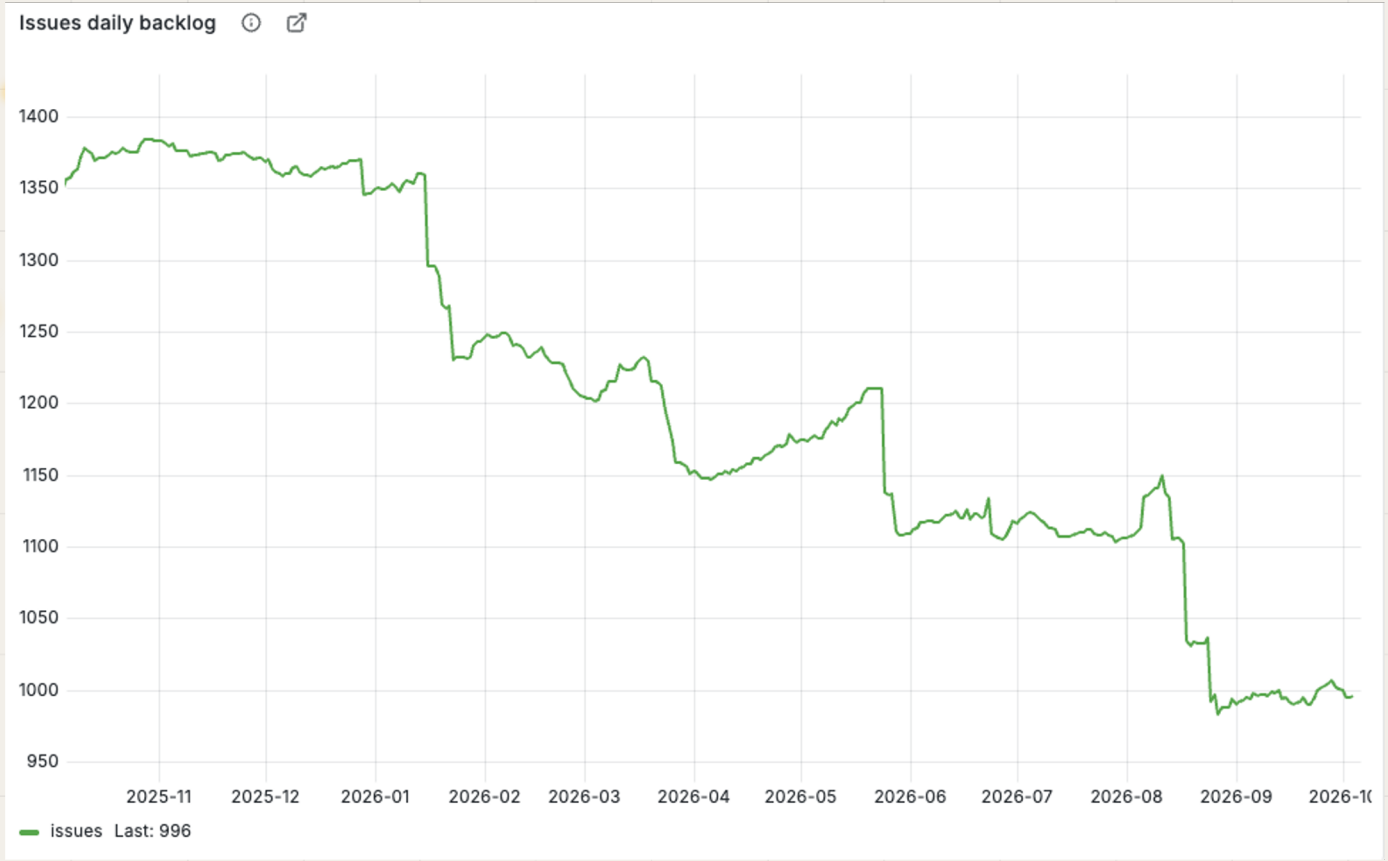
The Two Core Requirements

If a non-trivial portion of your submission has been created using an AI tool, you must:

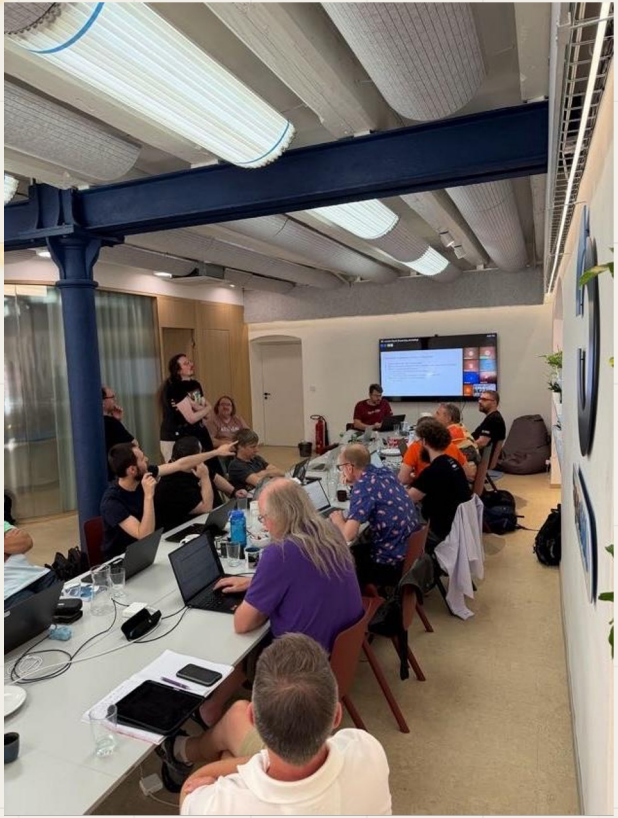
1. declare it in your commit message using an `Assisted-by` trailer, and
2. have signed a Contributor License Agreement (CLA) that includes the AI clauses.

Both requirements apply together. Neither alone is sufficient.

Issues backlog



Academics





Foundation Scholars



Award Abstract # 2625318

NSF Safe-OSE: Addressing Vulnerabilities in OpenSSL's Providers, Primitives, and Protocols

Total Intended Award Amount:	$1,498,710.00



Jose Luis Gonzalez



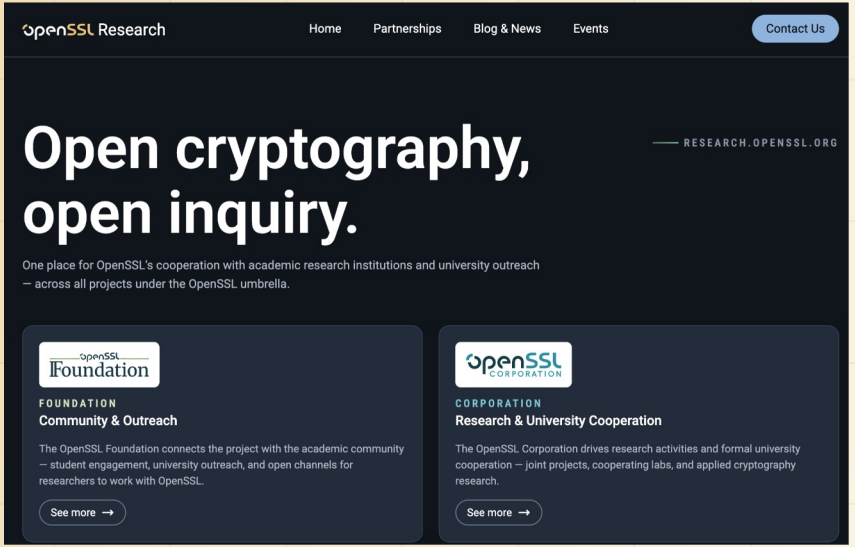
CSEC-535 — **Open Source Software Security** 3 Credits

The Free and Open-Source Software (FOSS) movement promotes the principles of software freedom, collaboration, and innovation, allowing users to access, modify, and share software without restrictions. FOSS is good for software security because it promotes transparency, allowing anyone to review the source code for vulnerabilities and ensuring that security flaws are more likely to be discovered and fixed quickly: "given enough eyeballs, all bugs are shallow" –Eric S. Raymond (Linus's law) In this course, we use OpenSSL—one of the most security-critical FOSS projects of our time—as a case study on the evolution of an FOSS project in response to vulnerabilities reported by security researchers. We study, discuss, and present their discovery, potential exploitation, mitigation, and to effectively contribute to FOSS projects.

RIT students tackle OpenSSL issues to help keep the internet encrypted

Open-source security course allows students to contribute to real-world cybersecurity





MUNI
FI

CROCS
Centre for Research on
Cryptography and Security

FIT
Security@FIT

Distributions

`3.5` LTS to 2030 · `3.6` non-LTS · `4.0` newest / pre-release · separate not in the base OS

Distribution	Latest release	OpenSSL
Nexbridge HPE NonStop port, via ITUGLIB	Tracks upstream branches	separate package
Chainguard Wolfi / Chainguard OS	Rolling	`3.6.5` `4.0 opt-in`
Ubuntu	26.04 LTS 26.10 in development	`3.5.5` `4.0.1`
SUSE	SLES 16.0	`3.5.0*`
Fedora	44 45 in testing	`3.5.7` `4.0.2`
Red Hat	RHEL 10.2 and 9.8	`3.5.5`
FreeBSD base system	15.1 (Jun 2026)	`3.5.x`
CentOS	Stream 10	`3.5.5`
Windows uses Schannel natively	Windows 11 25H2 26H2 in Release Preview	separate package

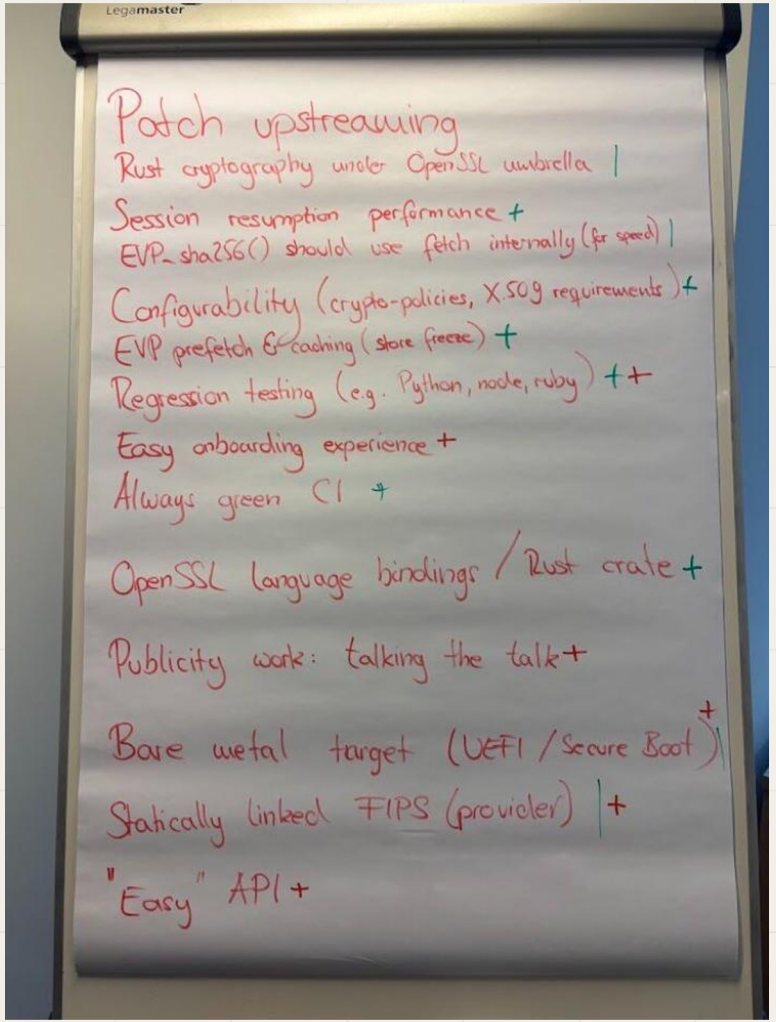
* Base version stays fixed; SUSE backports security fixes into it.



Results	Option	% of points	Points	Mean	Voters
	Regression testing (e.g. Python, Node, Ruby)	15%	6	0.67	9
	Patch upstreaming	15%	6	0.67	9
	Configurability (crypto-policies, x509 requirements)	15%	6	0.67	9
	EVP_sha256() should use fetch internally (for speed)	12%	5	0.56	9
	Session resumption performance	10%	4	0.44	9
	Publicity work: talking the talk	10%	4	0.44	9

FOSSDEM F2F 2026





DTLS 1.3 initial work - Small Business



Large Businesses



COMMUNITY SPOTLIGHT

The Large Business Community (LBC)

Run by Jeff Johnson (Cisco) — also the community's BAC delegate



Who's on the call?

cisco · HPE · aws · NetApp · Red Hat · CITRIX · ENTRUST

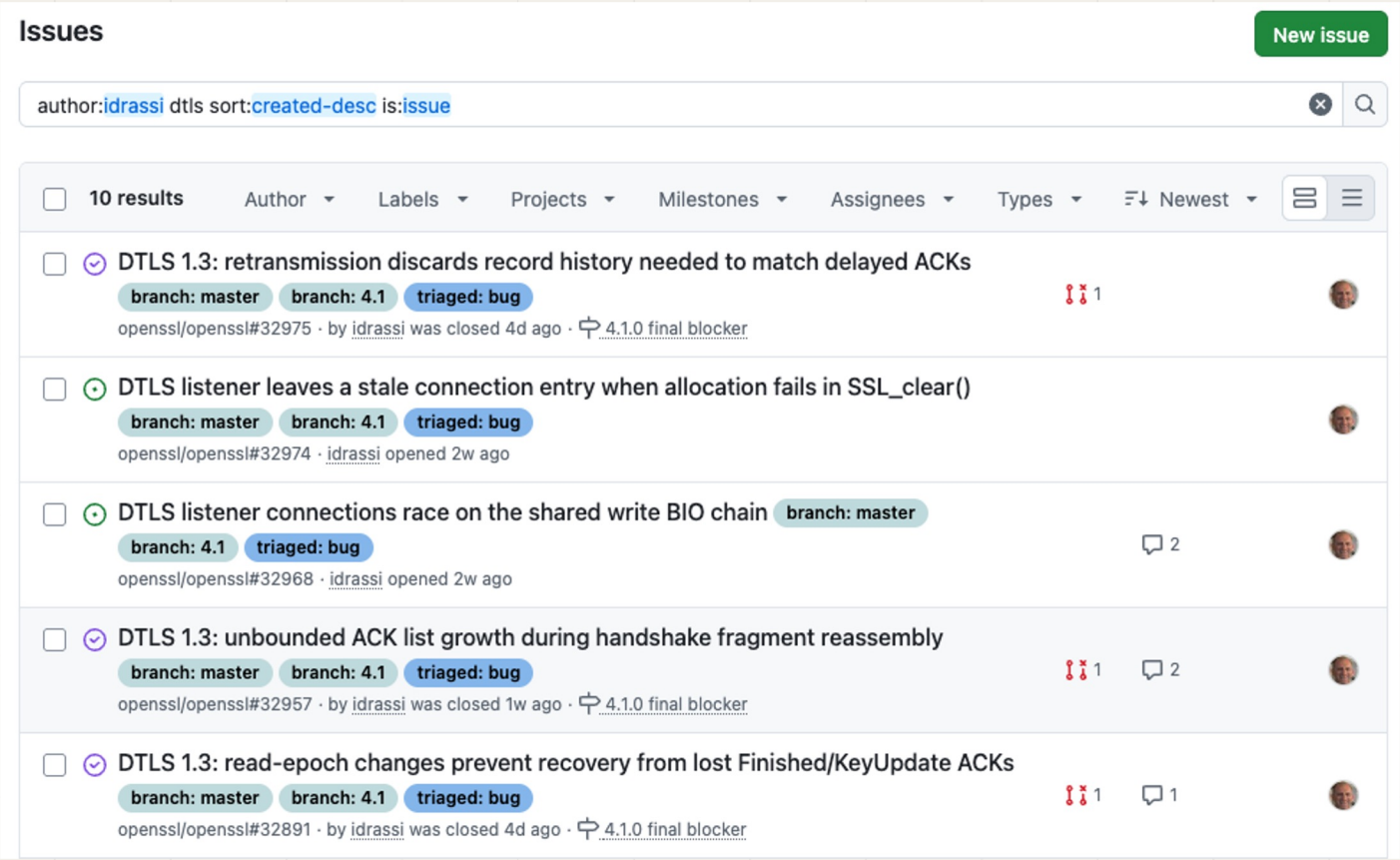
What's on the Agenda?

DTLS 1.3, QUIC API, FIPS 3.1 Support

Policy, performance improvements

§ Source: openssl-communities.org, hub-businesses-large (live) · discussion history via same connector

DTLS 1.3 testing - Individual



COMMUNITY SEAT

Small Businesses

Small businesses running or depending on OpenSSL in production — the seat currently sitting empty.

DELEGATES

BAC DELEGATE
— Vacant

TAC DELEGATE
— Vacant

METRICS · N/A

No delegate means no committee-reported metrics for this seat yet.

CHARTER

Represents small businesses running or depending on OpenSSL — distinct from the Large Businesses seat, and currently vacant on both committees.

INITIATIVES · GET OUT THE VOTE

We're asking at least three small-business owners to nominate themselves — next slide.

§ Source: openssl-corporation.org/community-committees.html

Be a delegate

Why?

Governance: Represent your community
Change: Shape ecosystem strategy & governance
Network: Direct channel to OpenSSL leadership

The PEOPLE & PLACES

DEV CONF
ICMC 2026
All Things Open
THE LINUX FOUNDATION OPEN SOURCE SUMMIT EUROPE

The BENEFITS

Early Access: Direct line to breaking news, shipping, & code releases.
Committee Funding: Scholarships, discretionary budget (AC/BAC), internships, grants
Experience: Work alongside top talent from globally recognized and independent institutions



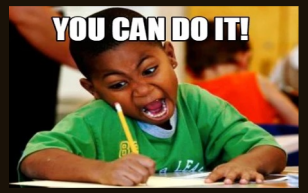




CTA: Replace complaints with results

Be heard. Protect the future. Join the OpenSSL Community!

It's in [y]our hands – distributions, committers, academics, businesses, individuals, and ...



NOMINATE YOURSELF OR A PEER openssl-communities.org — Corporation BAC / TAC hubs

Thank you to our leading supporters!

PREMIER SUPPORTERS

OpenSSL CORPORATION

CISCO

OPEN TECHNOLOGY FUND

Sovereign Tech Fund

nominet

CODE PROTECTORS

aws

craig newmark philanthropies

NetApp

OpenSSL Foundation

OpenSSL CONFERENCE

The State of the OpenSSL Community

THANK YOU FOR YOUR CONTRIBUTIONS!

https://openssl-communities.org