Summary of the year

July 2025 - July 2026

Paul Wouters and Tuomo Soini

The IPsec Workshop 2026
July 16, Vienna

Table of Contents

Libreswan Year In Review

Releases (July 2025 – Jul 2026)

- v5.2 — Feb 2025
- v5.3 — Jul 2025
- v5.3.1 — Jun 2026
- v5.3.2 — Jul 2026
- v5.4 — Jul 31 2026 *

Commits

- 2,350 non-merge commits

CVEs Issued

• CVE-2026-12413
OOB assertion in IKEv2 payload handling

• CVE-2026-50721
Truncated signed hash (IKEv1)

• CVE-2026-50722
Truncated signed hash (IKEv2)

• CVE-2026-14957
FIPS mode assertion failure
malicious CERT payload

Libreswan Major Topics / Development

New RFCs / Drafts Implemented

- RFC 9867 (PPK in IKE_INTERMEDIATE)
- RFC 9347 (IPTFS)
- RFC 9370 Multiple KE
  ADDKE and FOLLOWUP_KE
- draft-ietf-ipsecme-ikev2-mlkem
  (MLKEM hybrid+pure)

New Linux Features

- Handle outbound/inbound XFRM attributes for old/new kernels

Closing BSD-Linux Parity Gap

- On-demand
- IPsec-interface
- HOST-HOST

IKEv2 Features

- RFC 5723 IKE_SESSION_RESUME

IKEv1 Features

- Remove legacy hacks (eg softremote)
- Fix reconnecting clients using lease IP
- Improve IKE padding support
- Cisco split-net and share-lease fixups

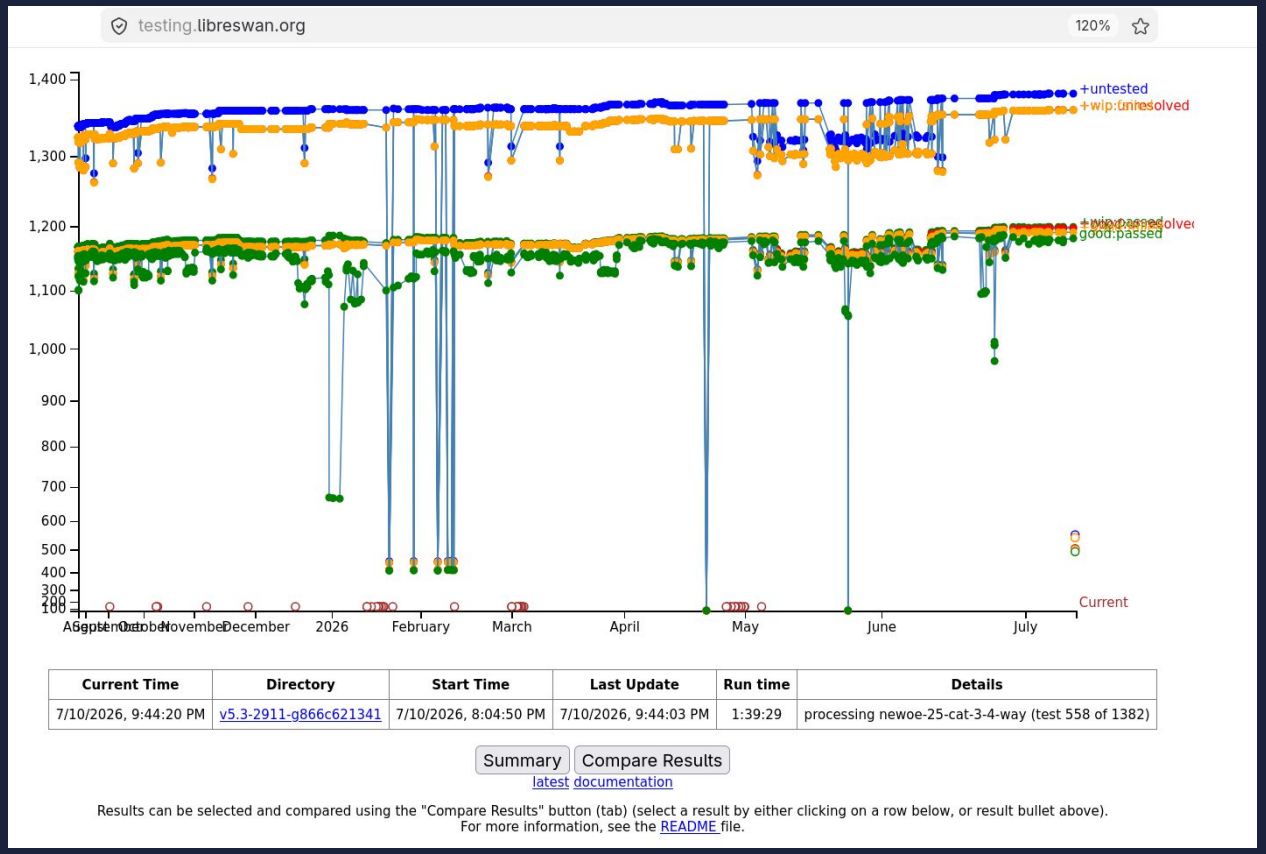
Libreswan Features

- Externally managed IPsec interfaces
- Connection loading speedups
- PKIX / CURL / LDAP cleanup, move code into NSS
- SA "crossing streams" improvements
- _stackmanager removed
- Logging improvements

Libreswan Testing at testing.libreswan.org

Building / Testing Highlights

- Many new BSD – Linux interop tests
- More test cases in general, now about 1,400 tests using multi VMs/namespaces
- All test runs going back years available at testing.libreswan.org



Google Summer of Code (GSoC) 2026

We suffered through a month of proposal hell — Thanks AI !

- 50 contacts, up from 5(?)
- Merged 24 pull requests during proposal period
- 4 Project Ideas, down from 15
- 30 proposals, up from 3(?) — 10 were pure A.I. slop
- But compared to other projects we had it easy.

Amrinder Singh
HOST-TO-HOST and On-Demand Support on the BSDs

Osema Fadhel
Announcing Authentication Methods (RFC 9593)

Vinayak Sandur
Optimising ACQUIRE message lookup time

libreswan

The Year of the AI vulnerabilities (and false positives)

We ran the libreswan code through a vulnerability analyses via Claude

Total cost: $27.95
Total duration (API): 1h 29m 41s
Total duration (wall): 6h 48m 49s
Total code changes: 2495 lines added, 99 lines removed
Usage by model:
claude-sonnet-4-6: 1.9k input, 303.1k output, 56.3m cache read, 1.7m cache write ($27.95)

CLAUDE	Claim:	Actual:
	4 High Severity	1
	10 Medium Severity	1
	10 Low Severity	5

Claude claims of High, Medium, Low scores

HIGH4 Claims

H1 alloc.c:319
Heap overflow in clone_bytes_bytes() (Indirect)

H2 ikev1_aggr.c:303 **[PoC]**
DoS: DH exhaustion + state flood (AGGR mode)

H3 ikev1_aggr.c:660 **[PoC]**
PSK offline crack via cleartext HASH_R (Passive)

H4 nss_cert_verify.c:413
PASSERT→abort via crafted CERT (FIPS only)

MEDIUM10 Claims

M1 x509dn.c: OOB read **[PoC]**
M2 x509.c: UAF derIssuer read
M3 ikev2_ike_sa_init.c: DH group steering
M4 ddos.c: Half-open SA flood
M5 lswalloc.h: alloc_things unchecked size
M6 alloc.c: key scrubbed 0xEF not zero
M7 ip_subnet.c: subnet wrong containment
M8 ikev2_ts.c: port ranges rejected
M9 secrets.c: NULL private key crash
M10 rcv_whack.c: PASSERT abort **[PoC]**

LOW10 Claims

L1 ikev1.c: MODE_CFG selected pre-decrypt
L2 ikev1.c: Fragment reassembly ≤1 MB/SA
L3 ikev1_quick.c: QM ID mismatch (MITM)
L4 ikev2_notification.c: unknown error ignored
L5 jambuf.c: array_as_jambuf underflow
L6 hunk.c: Signed overflow in raw_cmp
L7 ikev2_ts.c: selector mismatch TS widening
L8 ip_address.c: oversized input accepted
L9 secrets.c: PSK token in syslog **[PoC]**
L10 updown.c: PATH NULL crash on OpenBSD

Claude H4: A real problem assigned CVE-2026-14957

H4 ??? Remotely-triggered `abort()` via `PASSERT` in FIPS mode cert handling

File: programs/pluto/nss_cert_verify.c:413

```
if (is_fips_mode()) {
        SECKEYPublicKey *pk = CERT_ExtractPublicKey(cert);
        PASSERT(logger, pk != NULL);   // -> abort() if NSS returns NULL
```

CERT_ExtractPublicKey() returns `NULL` for certificates with malformed `subjectPublicKeyInfo` (unknown algorithm OID, zero-length BIT STRING, corrupt key encoding). `PASSERT` is declared `NEVER_RETURNS` ??? it kills pluto.

Trigger: Send a CERT payload containing a DER certificate that `CERT_NewTempCertificate()` accepts but `CERT_ExtractPublicKey()` rejects. One packet kills pluto on any FIPS-mode deployment.

Claude M2: x509.c UAF: freed cacert->derIssuer

M2 ??? Use-after-free: dangling shunk into freed `cacert->derIssuer`

File: programs/pluto/x509.c:237???248

```
asn1_t i_dn = same_secitem_as_shunk(cacert->derIssuer); // borrows cacert
match = same_dn(i_dn, b, verbose);
a = i_dn;                    // a aliases cacert->derIssuer.data
CERT_DestroyCertificate(cacert);  // frees the backing memory
cacert = NULL;
// next iteration: CERT_FindCertByName(handle, &a_dn) reads freed memory
```

The `shunk_t` is a non-owning borrow. `CERT_DestroyCertificate` frees the NSS arena containing `derIssuer.data`. The next loop iteration passes the dangling pointer to `CERT_FindCertByName`.

Reachable: Via `CERTREQ` payload in a deployment with intermediate CAs in the NSS database.

Libreswan Team analysis:

> call is a delref, not free. Crash would require local user to, in parallel, delete cert from db

Libreswan Roadmap 2026 / 2027

Libreswan Roadmap — Active Development

Actively Developed RFCs / Drafts

- draft-ietf-ipsecme-ikev2-mlkem — mostly merged
  Need to handle connection switching based on IKE_SA_INIT proposal
- RFC 9611 (per resource Child SA) — pull-request draft
- RFC 9593 (announce multiple AUTH) — GSoC 2026 project
- draft-pwouters-ipsecme-delete-info-04 — old branch, still under IETF discussion
- FOLLOWUP_KE, multi AUTH, PPK in IKE_INTERMEDIATE

On Our Radar to pick up next

- draft-ietf-ipsecme-child-pfs-info
- draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
- draft-ietf-ipsecme-eesp-ikev2
- IKEv2 Downgrade Prevention
- IKE parts of ESP ping / encrypted ping

Libreswan Roadmap — Desired / Future

Desired but Not Yet Planned or Started

- draft-guthrie-cnsa2-ipsec-profile
  Implement like fips? Per-connection param?
- draft-antony-ipsecme-ikev2-fragment-acknowledgment
  Under IETF discussion
- PQC authentication methods ???

Libreswan Roadmap — Work in Progress

Work in Progress

- Improve acquire / reqid handling
- BSD improvements related to acquire / on-demand

Other Code Features Planned

- Varlink support to replace whack
- Algorithm and PFS default settings update for 6.0
- Support for crypto-policies that does not use conn %default

Libreswan Roadmap — IKEv1 Support

Current Status

- IKEv1 code is compiled in by default but can be disabled
- IKEv1 connections are globally disabled by default
- Requires setting "config setup" option ikev1-policy=accept

Planned Changes

- libreswan 5.x — maintenance release remains unchanged
- libreswan 6.x (Q4 2026) — disable compiling IKEv1 by default
- libreswan 7.x (April 2027?) — removal of IKEv1 code

⚠️ **Requires coordination with strongSwan**

Tokenmaxxing: A libreswan rewrite in rust

Repository

- DO NOT USE - Almost no humans have looked at it !
- We ran is as a joke. It just worked much better than expected
- Private repo, access available, license unknown, not to be republished
- https://github.com/paulwouters/libreswan-rust

Current Status

- It compiles and it interops with libreswan showing non-zero traffic counters (!)
- IKEv2 only, it was told to not port IKEv1
- IKEv2 PSK tested, X.509 status unknown
- It uses the rust native crypto library instead of NSS
- It uses terraform deployment to AWS for deploy/interop tests

Cost

- Initial build cost $2,800 and was done by Guillaume Winter @ Aiven