

SECURITY FIX EVIDENCE PACK & REVIEW LEDGER

Prepared for Acme Payments Ltd (Demo Org) (acme) | Repository: acme/payments-api

1. Pack Provenance & Cryptographic Manifest (SHA-256 + Ed25519)

Evidence Pack ID:	pack_9797e9e7c985b5a6 (FINAL)
Organization:	acme (GitHub Owner ID: 99001122, Org ID: org_demo_acme)
Repository:	acme/payments-api
Generated At (UTC):	2026-10-24T16:52:57Z by sara-sec
Source Snapshot:	Ingest ing_9b751ae553c40707 (fixdossier/v1, 5371 bytes, auth=github_oidc)
Source Snapshot SHA-256:	91e237808f3644d30ee237009ec66bb4c9384c1d3efcbd3ca10e9184de003551
GitHub OIDC Provenance:	run_id=11492837412 commit=c82b17f492e80d14a9b8e31d9904c2b17a5f3210 ref=refs/tags/v2.4.2 w...
Reviewed Record SHA-256:	03ce08885879669c90deaca799a72885921b41e4c5f568b7bf33d4853e57f35e (security-record-reviewed.j...
Support Statement SHA-256:	9fa6ec7810dcc1b8eede914779b3a53d8c54bd984e6a743c1ff249ff6084e425 (SUPPORT.md)
Audit Trail Head Hash:	7c039454ca8068f6a4901b9166c1777ad07033a13740a6b49118b6a2f209dab3
Ed25519 Signing Key:	ed25519:0961c15ac1deac6c (PubKey: 0961c15ac1deac6cf20bf3671905c1e7a14d38b0813604aeb377a8a1b3...
Verification Endpoint:	POST https://app.fixdossier.dev/api/v1/verify (or offline Ed25519 verify against pack-manife...

2. Executive & Coverage Summary

Total Candidate Items: 7 Advisory-Derived: 3 Heuristic-Derived: 4 Releases Tracked: 4
Confirmed Security Fixes: 5 Excluded (Not Security): 1 Needs Follow-up: 1 Unreviewed: 0 Unmatched/Unreleased: 1

Recorded Collection / Permission Gaps:

- commits: inspected most recent 250 commits on default branch (raise max_pages for pre-2025 history)

3. Support-Period Statement & Vulnerability Reporting

Security updates for acme/payments-api are provided for each stable release for 18 months from its publication date, and in any case not after 2028-12-31 (end of life). Security vulnerabilities should be reported to security@acme-payments.example.

4. Legal & Methodology Disclaimer

IMPORTANT NOTICE: fixdossier Pro is a technical evidence collection and review support tool, not legal advice. It automatically collects candidate records from GitHub releases, tags, published GitHub security advisories, merged Dependabot/Renovate PRs, and keyword-matched commits, and records human engineering review decisions. It is not a complete vulnerability inventory and does not certify compliance with the EU Cyber Resilience Act (CRA), EU Product Liability Directive (PLD), or any other regulation. Cryptographic hashes and Ed25519 signatures verify file integrity since pack generation, not completeness or legal sufficiency.

5. Release Timeline & Support Window Status

Release Tag	Published	Support Until	Type	Commit SHA
v2.4.2	2026-10-18	2028-04-18	stable	c82b17f492e80d14
v2.4.1	2026-09-12	2028-03-12	stable	a71e93c284b10d42
v2.4.0	2026-08-03	2028-02-03	stable	f19d04a173c20e51
v2.3.0	2026-05-19	2027-11-19	stable	b08c93f062b10d40

6. Reviewed Security-Fix Ledger (With Reviewer Attribution & Timestamps)

[1] fix(xml): disable external entity resolution in legacy ISO-20... | Status: NEEDS_FOLLOWUP | Severity: HIGH | Release: UNRELEASED

Source: commit (heuristic, mapping: unreleased) | Date: 2026-10-22 | CVE/GHSA Notes: CVE-2026-44001 (merged to main, awaiting v2.4.3 tag)

Reviewer Sign-off: sara-sec at 2026-10-24T16:52:57Z (UTC)

Engineering Rationale: Fix is merged on main (commit 9e88f1c2) but not yet tagged in a release. Cut v2.4.3 release before final customer attestation.

[2] Timing side-channel in webhook HMAC signature verification al... | Status: CONFIRMED_SECURITY_FIX | Severity: HIGH | Release: UNRELEASED

Source: advisory (advisory, mapping: advisory patched_versions) | Date: 2026-10-18 | CVE/GHSA Notes: GHSA-9f4c-7q2x-p8m1, CVE-2026-41892

Reviewer Sign-off: sara-sec at 2026-10-24T16:52:57Z (UTC)

Engineering Rationale: Replaced byte-by-byte string equality check with constant-time hmac.Equal in webhook middleware. Shipped in v2.4.2.

[3] fix(auth): enforce strict PKCE S256 verifier length to preven... | Status: CONFIRMED_SECURITY_FIX | Severity: MEDIUM | Release: UNRELEASED

Source: commit (heuristic, mapping: date heuristic (first release on/after commit)) | Date: 2026-10-16 | CVE/GHSA Notes: Internal audit finding SEC-2026-19

Reviewer Sign-off: mikael-dev at 2026-10-24T16:52:57Z (UTC)

Engineering Rationale: Hardened OAuth2 PKCE verifier validation to reject plain challenge method and <43 char verifiers. Shipped in v2.4.2.

[4] chore(deps): bump golang.org/x/crypto from 0.27.0 to 0.29.0 (... | Status: CONFIRMED_SECURITY_FIX | Severity: MEDIUM | Release: UNRELEASED

Source: dependency-update (heuristic, mapping: date heuristic (first release on/after merge)) | Date: 2026-10-14 | CVE/GHSA Notes: CVE-2026-39112, GHSA-

Reviewer Sign-off: sara-sec at 2026-10-24T16:52:57Z (UTC)

Engineering Rationale: Dependabot bump of golang.org/x/crypto to 0.29.0 remediates SSH packet parsing DoS in SFTP reconciliation worker.

[5] SSRF in merchant webhook callback URL validator via IPv4-mapp... | Status: CONFIRMED_SECURITY_FIX | Severity: CRITICAL | Release: UNRELEASED

Source: advisory (advisory, mapping: advisory patched_versions) | Date: 2026-09-11 | CVE/GHSA Notes: GHSA-3v8x-k92p-4w6r, CVE-2026-38410

Reviewer Sign-off: sara-sec at 2026-10-24T16:52:57Z (UTC)

Engineering Rationale: Blocked IPv4-mapped IPv6 private/loopback prefixes in custom dialer before outbound webhook dispatch. Verified in v2.4.1.

[6] Missing tenant scope check on batch payout CSV export endpoint | Status: CONFIRMED_SECURITY_FIX | Severity: HIGH | Release: UNRELEASED

Source: advisory (advisory, mapping: advisory patched_versions) | Date: 2026-08-01 | CVE/GHSA Notes: GHSA-6p5m-2c7q-8x9n

Reviewer Sign-off: mikael-dev at 2026-10-24T16:52:57Z (UTC)

Engineering Rationale: Enforced mandatory WithOrg(orgID) scoping on batch CSV export query. Shipped in v2.4.0.

7. Unmatched & Excluded Items (With Engineering Reasons)

[1] UNMATCHED / UNRELEASED IN SNAPSHOT " fix(xml): disable external entity resolution in legacy ISO-20022 pars... (Date: 2026-10-22, Source: commit)

Reason / Notes: Fix is merged on main (commit 9e88f1c2) but not yet tagged in a release. Cut v2.4.3 release before final customer attestation.

(Reviewer: sara-sec, Reviewed At: 2026-10-24T16:52:57Z)

[2] EXCLUDED (Not a security fix) " refactor(security-headers): rename internal security middleware helper (Date: 2026-09-02, Source: commit)

Reason / Notes: Pure internal function rename with zero behavior change. Matched commit heuristic due to 'security' in scope name. (Reviewer:

mikael-dev, Reviewed At: 2026-10-24T16:52:57Z)

8. Append-Only Review Audit Trail & Signature Verification

#7	2026-10-24T16:52:57Z	actor=mikael-dev	item=item_4601e840ad0d6f96	unreviewed -> confirmed_security_fix	hash=7c039454ca806
#6	2026-10-24T16:52:57Z	actor=mikael-dev	item=item_a930a5719eb7b331	unreviewed -> excluded_not_security	hash=d77df3a07c9db.
#5	2026-10-24T16:52:57Z	actor=sara-sec	item=item_7490a4d1aa63eb00	unreviewed -> confirmed_security_fix	hash=a6b4b8816792a..
#4	2026-10-24T16:52:57Z	actor=sara-sec	item=item_566a03642b9d6916	unreviewed -> confirmed_security_fix	hash=e74a24e4d10f4..
#3	2026-10-24T16:52:57Z	actor=mikael-dev	item=item_1d98c474cc23a981	unreviewed -> confirmed_security_fix	hash=595e75f1961a1.
#2	2026-10-24T16:52:57Z	actor=sara-sec	item=item_140c6ca577e122a6	unreviewed -> confirmed_security_fix	hash=868925dea3512..
#1	2026-10-24T16:52:57Z	actor=sara-sec	item=item_3b2bd650c0517424	unreviewed -> needs_followup	hash=3a5ce641d7278...

How to Verify This Evidence Pack:

1. Check SHA-256 digests of evidence-pack-*.pdf, security-record-reviewed.json, and SUPPORT.md against pack-manifest.json.
2. Verify the Ed25519 signature over the canonical manifest payload using public key
0961c15ac1deac6cf20bf3671905c1e7a14d38b0813604aeb377a8a1b3a408da
or POST pack-manifest.json to <https://app.fixdossier.dev/api/v1/verify>.