KANAME SECURITY

Ref KS-20261127-7465
Scanned 2026-11-27 14:38 UTC
Classification Confidential

POST-QUANTUM READINESS REPORT

example.com

01 Summary

67
/ 100 · C

Edge-only hybrid PQ

At Risk · The CDN edge negotiated hybrid PQ; the origin leg is unverified.

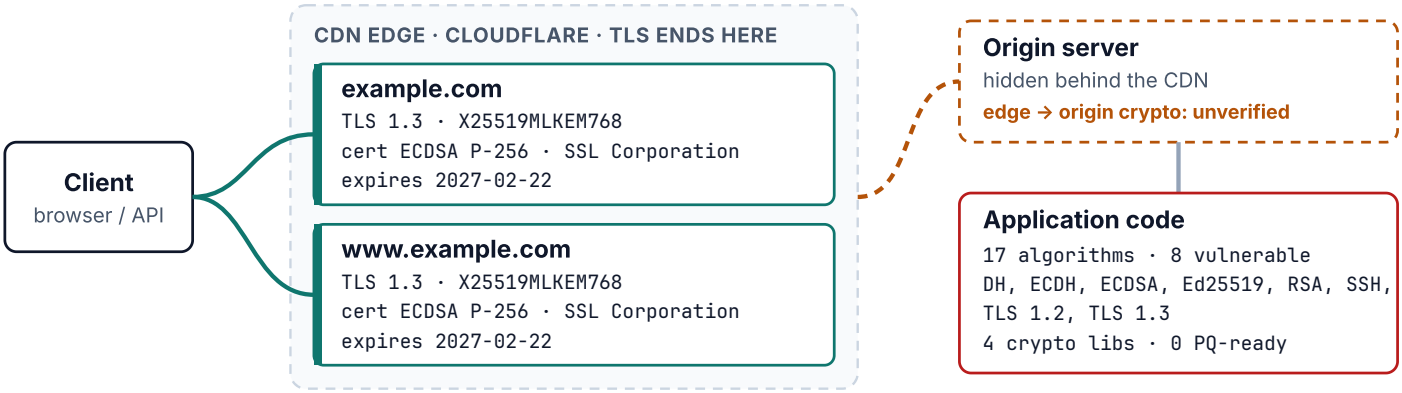
Transport Protocol	TLS 1.3
Key exchange	X25519MLKEM768 · Hybrid PQ
Certificate public key	ECDSA P-256
Origin visibility	Masked by Cloudflare

TOP GAPS

- HIGH — 6 quantum-vulnerable algorithms in code
- HIGH — Broken or deprecated primitives in use: MD5, SHA-1
- HIGH — Post-quantum key exchange stops at the edge; origin leg is classical
- HIGH — Plain HTTP is not redirected to HTTPS

0	4	3	4	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

02 Observed architecture



DNS TRUST
DNSSEC ECDSA P-256 · validated · no CAA

CERTIFICATE STATUS
OCSP good · CRL fresh · stapling observed

hybrid post-quantum — classical / quantum-vulnerable — unverified — not assessed

LAYER	OBSERVED	STATUS
Key exchange (client ↔ edge)	X25519MLKEM768	Quantum-safe
Key exchange (edge ↔ origin)	Not visible from outside	Not verified
Certificate signature	ECDSA P-256	Quantum-vulnerable

LAYER	OBSERVED	STATUS
Bulk encryption	`TLS_AES_256_GCM_SHA384`	Quantum-safe
Protocol fallback	`TLS 1.2 still accepted (no PQ possible)`	Weakened
DNSSEC signing	`ECDSA P-256`	Quantum-vulnerable
Application code	`DH, ECDH, ECDSA, Ed25519, RSA, SSH, TLS 1.2, TLS 1.3`	Quantum-vulnerable
Application code (weak)	`AES, AES-128, MD5, SHA-1`	Weakened

03 Findings (13)

SEVERITY	FINDING	FIX
HIGH CBOM-001	**6 quantum-vulnerable algorithms in code** **Evidence** DH, ECDH, ECDSA, Ed25519, RSA, SSH. 15 call sites across 4 files. **Impact** Public-key operations in code will need an algorithm swap.	Introduce a crypto-agility abstraction at these call sites, then migrate KEM/key-agreement paths to ML-KEM first (highest HNDL exposure), signatures second. Medium-Large (per call site) · Engineering
HIGH CBOM-002	**Broken or deprecated primitives in use: MD5, SHA-1** **Evidence** Detected in source across 4 languages. **Impact** These fail classical security today, before quantum is a factor.	Replace with SHA-256/SHA-3 and AES-GCM or ChaCha20-Poly1305. Small per site, but breaks stored hashes and on-disk formats · Engineering
HIGH KEX-002	**Post-quantum key exchange stops at the edge; origin leg is classical** **Evidence** Cloudflare terminates TLS with X25519MLKEM768. Origin visibility: masked. **Impact** The client-to-edge hop is protected, but edge-to-origin traffic is still classical.	Extend hybrid key exchange to the origin terminator and pin the connection with mTLS or an origin-side PQ-capable tunnel. Re-test with the edge bypassed. Medium (1-2 weeks) · Platform / Network
HIGH TRN-001	**Plain HTTP is not redirected to HTTPS** **Evidence** http://example.com returned 200 without an HTTPS Location header. **Impact** The first request is sent in the clear and can be hijacked before any TLS protection applies.	Return 301/308 to the HTTPS origin for all plaintext requests at the edge. Trivial · Platform / Network
MEDIUM DNS-001	**No CAA record: any CA may issue for this domain** **Evidence** CAA lookup returned 0 records. **Impact** A mis-issuing or compromised CA can mint a valid certificate for your domain;	Publish `CAA 0 issue "letsencrypt.org"` (and your other CAs) plus `CAA 0 iodef "mailto:security@..."`. Trivial · DNS / Platform
MEDIUM TRN-002	**No HSTS policy** **Evidence** Strict-Transport-Security header absent on the HTTPS response. **Impact** Browsers will happily follow a downgrade on the next visit, so the TLS work above can be bypassed.	Send `Strict-Transport-Security: max-age=31536000; includeSubDomains` after confirming all subdomains are HTTPS-only. Trivial · Platform / Network

SEVERITY	FINDING	FIX
MEDIUM VIS-001	**Origin is masked by a CDN, so true origin cryptography is unverifiable from outside** **Evidence** cf-ray: a611e03d5925252c-SIN; server: cloudflare; cf-cache-status: HIT. **Impact** An external scan cannot distinguish 'PQ everywhere' from 'PQ at the edge only'.	Run an internal or origin-side assessment (this tool's repo/CBOM mode plus an authenticated origin probe) and record the origin terminator explicitly in your CBOM. Low (test), Medium (remediation) · Platform / Network
LOW SIG-001	**Certificate uses a quantum-vulnerable signature (ECDSA P-256)** **Evidence** Issuer SSL Corporation; valid 2026-11-24T23:48:34Z → 2027-02-22T23:53:08Z (90 days). **Impact** Forgery of the certificate becomes feasible for an adversary with a quantum computer, enabling impersonation.	Shorten certificate lifetime to ≤90 days, automate renewal (ACME), and inventory every place the key is deployed so a future swap to ML-DSA is a config change rather than a project. Low · PKI / Platform
LOW TRN-003	**TLS 1.2 still accepted, widening the downgrade surface** **Evidence** TLS 1.2 handshake succeeded alongside TLS 1.3. **Impact** PQ hybrid groups are TLS 1.3-only;	Disable TLS 1.0/1.1 immediately and schedule TLS 1.2 removal once client telemetry permits. Low · Platform / Network
LOW TRN-004	**No Content Security Policy** **Evidence** Neither Content-Security-Policy nor a report-only policy was observed. **Impact** Weakens defence against script injection, which is how session tokens and keys get stolen in practice.	Start in report-only with `default-src 'self'`, collect violations for two weeks, then enforce. Low · Application
LOW TRN-005	**No anti-framing control** **Evidence** Neither X-Frame-Options nor CSP frame-ancestors is set. **Impact** Enables clickjacking of authenticated actions.	Set `X-Frame-Options: DENY` or CSP `frame-ancestors 'none'`. Trivial · Application
INFO DNS-003	**DNSSEC signing keys are classical (no PQ DNSSEC algorithm standardised yet)** **Evidence** DNSKEY algorithms in use: 13 (RSA/ECDSA). **Impact** DNSSEC authenticity will itself need migration;	Track the IETF DNSSEC PQ work and keep the zone signing key short-lived so migration is routine. None today · DNS / Platform
INFO TRN-006	**MIME sniffing protection not set** **Evidence** X-Content-Type-Options absent. **Impact** Browsers may reinterpret a response as executable content.	Send `X-Content-Type-Options: nosniff`. Trivial · Application

04 Action plan

NOW — 0-6 months

Stop the bleeding: key exchange and spoofing

1. Extend hybrid key exchange to the origin terminator and pin the connection with mTLS or an origin-side PQ-capable tunnel. Re-test with the edge bypassed.
2. Return 301/308 to the HTTPS origin for all plaintext requests at the edge.

Done when All public endpoints negotiate a hybrid PQ group; no critical finding remains open.

NEXT — 6-18 months

Depth: origin, internal paths, and agility

1. Publish `CAA 0 issue "letsencrypt.org"` (and your other CAs) plus `CAA 0 iodef "mailto:security@..."`.
2. Send `Strict-Transport-Security: max-age=31536000; includeSubDomains` after confirming all subdomains are HTTPS-only.
3. Run an internal or origin-side assessment (this tool's repo/CBOM mode plus an authenticated origin probe) and record the origin terminator explicitly in your CBOM.

Done when CBOM covers every internet-facing and tier-1 internal crypto dependency.

LATER — 18-36 months

Signatures and steady state

1. Shorten certificate lifetime to ≤90 days, automate renewal (ACME), and inventory every place the key is deployed so a future swap to ML-DSA is a config change rather than a project.
2. Disable TLS 1.0/1.1 immediately and schedule TLS 1.2 removal once client telemetry permits.
3. Start in report-only with `default-src 'self'`, collect violations for two weeks, then enforce.
4. Set `X-Frame-Options: DENY` or CSP `frame-ancestors 'none'`.
5. Plan the ML-DSA certificate migration: confirm CA roadmap, test hybrid signature support in your terminators, and keep the key inventory current so the swap is a configuration change.
6. Add cryptographic inventory to the SDLC: a CBOM diff on every release, gating on new classical algorithms.

Done when Signature migration plan approved, certificate lifetimes ≤90 days, CBOM drift alerts live.

05 Score breakdown · 67/100

Key exchange (HNDL)	24/35	Hybrid key exchange terminates at the CDN edge;
Signatures & certificates	9/20	ECDSA P-256 signatures are quantum-vulnerable;
Estate coverage	15/15	2 of 2 tested hosts negotiate PQ.
Transport hardening	4/12	TLS versions: TLSv1.3;
Crypto-agility operations	7/10	Revocation reachability, CAA pinning and DNSSEC together determine how safely you can swa...
Email authentication	8/8	Email is where identity phishing lands;

EVIDENCE

Transport & Identity — PQ READY

TLS protocol	TLS 1.3
Key exchange	X25519 + ML-KEM-768
Certificate key	ECDSA P-256
Endpoint consistency	Consistent
HTTP/3 / QUIC PQ status	Alt-Svc advertises h3; PQ unverified
Cipher suite	TLS_AES_256_GCM_SHA384
Certificate issuer	SSL Corporation
Certificate managed by	Cloudflare
Certificate expiry	2027-02-22 · 87 days
Standards alignment	Hybrid KEX per NIST IR 8547

Email authentication — GOOD

SPF policy	-all · hard fail
DKIM public key	default · key present
DMARC policy	p=reject
Policy coverage	pct=100
Subdomain policy	sp=reject

Web security headers — MISSING

HTTP → HTTPS	No redirect
HSTS	Not observed
Content Security Policy	Not observed
Anti-framing policy	Not observed
MIME sniffing	Not observed

DNS trust & issuance — INCOMPLETE

Parent DS record	Present
DNSKEY record	ECDSA P-256 · classical
Authenticated delegation	Established
CAA policy	Any CA may issue
Quantum-resistant DNS	No PQ DNSSEC algorithm standardised yet

Certificate revocation — GOOD

OCSP responder	Good · 1 URL(s)
OCSP stapling	Observed
CRL	Fresh · next update 2026-12-04

06 Code cryptography (CBOM)

17	8	4	15	10	0
ALGORITHMS	VULNERABLE	WEAKENED	VULNERABLE CALL SITES	DEPENDENCIES	EMBEDDED SECRETS

ALGORITHM	FAMILY	STATUS	SITES
SHA-256	hash	Quantum-safe	5
AES-256	symmetric	Quantum-safe	3
ECDH	asymmetric	Quantum-vulnerable	3
SSH	protocol	Quantum-vulnerable	3
RSA	asymmetric	Quantum-vulnerable	3
ECDSA	asymmetric	Quantum-vulnerable	2
SHA-1	hash	Weakened	2
AES-128	symmetric	Weakened	1
SHA-384	hash	Quantum-safe	1
TLS 1.2	protocol	Quantum-vulnerable	1
TLS 1.3	protocol	Quantum-vulnerable	1
ChaCha20-Poly1305	symmetric	Quantum-safe	1

CRYPTO LIBRARY	VERSION	PQ SUPPORT
helmet	7.1.0	Quantum-vulnerable
jsonwebtoken	9.0.2	Quantum-vulnerable
node-forge	1.3.1	Quantum-vulnerable
cryptography	42.0.5	Weakened

07 Scope and limits

- Passive scan of public endpoints: TLS 1.3 PQ-first and classical handshakes, certificate chain, revocation, HTTP headers, DNS (DNSSEC, CAA, SPF, DKIM, DMARC), plus a static repository inventory.
- No crawling, authentication, fuzzing or exploitation.
- A CDN hides the origin. Edge-only PQ is reported as edge-only, never as end-to-end.
- Point-in-time result. Absence of a finding is not proof of absence.
- Score: key exchange 35 · signatures 20 · estate coverage 15 · transport 12 · crypto-agility 10 · email 8.
- Reproducible from report.json. OpenSSL 3.6.3 · PQ groups X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024, MLKEM768.