PATERO

POWERED BY nQrypt

CRYPTOGRAPHIC ECOSYSTEM MANAGEMENT
quantumsafe@patero.io · (650) 678-0678 · www.patero.io

BLACK OCTOBER 2026

Patched is not closed. The day-two checklist.

Between October 17 and 22, PHP2Shell (CVE-2026-109618 / 109619), the GitLab CVSS 10.0 RCE, the LiteLLM 1.107.0 malicious release, the Railway and Zeabur intrusions and the eMudhra weak intermediate-CA keys were disclosed within days of each other. Every vendor fix is a patch, a revocation or a clean release. None of them touches what the compromised system already held.

What stays open is the same in every case: the certificates, private keys, signing material and trust relationships that were reachable from the exposed system, and whether every one of them has been reissued. A patch stops the next exploit. It does not revoke a key that was readable last Tuesday, and it does not update a trust store on a device that never takes browser updates.

Four questions. If any takes more than a day to answer, the inventory does not exist yet.

01 Scope — what was reachable

- [ ] Every host that ran an affected PHP, GitLab, Node.js or Plex version while internet-reachable, with dates exposed
- [ ] Every environment that pulled LiteLLM 1.107.0, the OVHcloud CLI Oct 19 binaries or Rank Math PRO 3.0.123 in the affected windows
- [ ] Every certificate, private key, signing key and keystore that lived on those hosts or in those environments
- [ ] Apache mod_php hosts flagged separately: PHP ran inside the httpd worker, the same process that holds mod_ssl key material

02 Dependencies — what else trusts it

- [ ] For each key: what authenticates with it — internal CAs, mTLS peers, service-to-service calls, device enrollment, code signing
- [ ] Every system that chains to or pins the eight revoked eMudhra intermediates, including Operational Technology, embedded and IoT devices that never receive browser trust-store updates
- [ ] For platform-held secrets (Railway, Zeabur, OpenCode Console): what each exposed key could reach beyond the platform

03 Rotation — what has actually been reissued

- [ ] Reissue every certificate and key from step 1; revoke the old ones
- [ ] Replace trust anchors on every system from step 2, including the ones with no update channel
- [ ] Rotate every platform secret from step 1, including any already "rotated" after an earlier incident

04 Proof — show it closed

- [ ] Confirm the old key no longer authenticates anywhere — live, not by ticket status
- [ ] Confirm no system still trusts the revoked intermediates
- [ ] Produce an attestation with provenance: what was found, what changed, when, by whom, verified against what

Step 4 is not optional. Zeabur's own investigation found credentials left valid after its August 2026 incident because rotation was incomplete; those credentials were used in the October intrusion. LiteLLM's root cause was a key exposed in May, corrected in the repository, and never revoked.

Incident by incident — the vendor fix, and the question it leaves behind

Incident (disclosed)	Vendor fix	Cryptographic day-two question
PHP2Shell CVE-2026-109618 / 109619 (Oct 21)	PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35	Which certs and keys lived on exposed hosts, especially mod_php, and what still trusts them?
eMudhra weak P-384 intermediates (Oct 17)	Eight intermediates revoked; browser trust stores updated	Which of our systems, including OT and embedded devices, still chain to or pin those intermediates?
LiteLLM 1.107.0 malicious release (Oct 21)	Release pulled; rebuild affected environments	Which signing keys and credentials were reachable from environments that ran it, and is their provenance intact?
Railway secrets exposure (Oct 22)	Attacker removed; customers told to rotate	Which keys were stored there, what else do they reach, has every one been rotated?
Zeabur credential reuse (Oct 19)	Credentials reset	Did rotation after the last incident actually complete, and can we show it?
GitLab CVE-2026-110264 (Oct 21)	Patch 19.5.1	Which deployment tokens and signing keys lived in affected self-managed instances?
Node.js TLS hostname-validation flaws (Oct 21)	22.23.4, 24.22.1, 26.12.1	Which workloads run an affected TLS stack, and which bundle it separately?

The PHP memory-disclosure point is an exposure assumption, not an observed theft: researchers demonstrated remote code execution and disclosure of process memory, and standard incident practice treats key material on a host with unauthenticated RCE as compromised.

What Patero, powered by nQrypt, does here — and does not

Patero, powered by nQrypt, answers steps 1 through 4 from an inventory it builds, not one it is handed: certificates, keys, signing material and cryptographic implementations across IT and Operational Technology, every chain mapped to its root including private and internal CAs, and what depends on what. Metadata only. **A private key is never collected or transported.**

Step	Does	Does not
01 Scope	Lists the certificates, keys and crypto implementations on each host, workload and device, with where they live	Patch PHP, GitLab or Node.js; detect the exploit itself
02 Dependencies	Maps chain-to-root and the relationships between cryptographic uses; matches trust stores on OT and embedded devices against the revoked eMudhra intermediates	Replace a WAF, EDR or vulnerability scanner
03 Rotation	Drives reissuance and trust-anchor replacement through your existing CLM, PKI and device tooling	Remove malware or persistence left by an exploit
04 Proof	Validates live that old material no longer authenticates and nothing still trusts it; produces an attestation with full provenance	Guarantee a secret stored outside its discovered scope was rotated

The same inventory covers users, devices, workloads and AI agents, which is why Railway, OpenCode and LiteLLM sit on the same checklist as PHP2Shell and eMudhra: the question is what cryptographic material the compromised environment could reach, and the answer comes from the same map. Non-disruptive on operational networks. Reports against BOM, CBOM, XBOM and ML-BOM, so the step-4 attestation is the artifact auditors and the budget owner read.

Next step. A scoped proof-of-concept on the hosts and devices you already know were exposed. Day one: discover what cryptographic material sat on them and what depends on it. Day two: reissuance driven and validated live, and an attestation with provenance in hand for that scope. The full-estate roadmap comes after the proof, not before it.

Start the conversation: quantumsafe@patero.io · (650) 678-0678 · www.patero.io

Sources: Black October roundup (Unosecur, Oct 26) · PHP2Shell (Wikipedia) · NCSC-NL php2shell · LiteLLM attack-chain investigation · Railway preliminary report · Zeabur incident report. As of October 27, 2026.