

SECURITY ADVISORY

eMudhra Intermediate CA Certificate Key Compromise

Weak certificate-authority keys create potential website impersonation and software-signing risks.

SEVERITY	PUBLISHED	CATEGORY	STATUS
HIGH	23 OCT 2026	PKI / TLS	MITIGATION ACTIVE
IMPORTANT DISTINCTION This is a cryptographic certificate-authority security incident, not a confirmed data breach. eMudhra says its infrastructure and customer data were not breached; its India DSC and eSign operations are unaffected. [1, 2]			

01 INCIDENT SUMMARY

On 17 October 2026, a security researcher disclosed that private keys for eight eMudhra (emSign) intermediate Certificate Authorities (CAs)—six TLS and two code-signing—could be recovered because they were generated with extremely weak randomness. The keys originated in an April 2025 key-generation ceremony. An attacker could use a recovered CA key to create fraudulent certificates where clients still trust the affected chain. [1–4]

eMudhra revoked the eight intermediate CAs on 18 October. According to eMudhra, none of the eight issued end-entity certificates and the root CA private keys were not compromised. Public reporting has not established malicious exploitation of the weak keys as of this advisory. [1, 2]

08	06 + 02	18 OCT
Affected intermediate CAs	TLS + code-signing CAs	Certificates revoked

02 POTENTIAL IMPACT

TLS impersonation — On clients that still accept compromised CA chains, a network-positioned attacker could present fraudulent HTTPS certificates and potentially read or alter traffic.

Code-signing abuse — Compromised code-signing CA keys could support issuance of fraudulent code-signing certificates.

Service disruption — Removal of emSign ECC Root CA - G3 from trust stores may break legitimate TLS connections that chain to that root, even when those leaf certificates were not issued by the compromised intermediates. [1, 3]

03 PRIORITY ACTIONS FOR CUSTOMERS

- 1. **Inventory certificate chains.** Identify websites, load balancers, APIs and mTLS services using the emSign ECC Root CA - G3 chain or affected emSign intermediate CAs. Include externally supplied services.
 - 2. **Replace affected TLS certificates.** Where certificates rely on the distrusted G3 root, migrate to a valid, independently trusted CA hierarchy before client distrust changes reach your users.
 - 3. **Patch trust stores and software.** Apply vendor browser, OS, runtime, appliance and container updates. Review software with its own CA bundle; redeploy where needed.
 - 4. **Validate and monitor.** Confirm affected chains are rejected, monitor certificate-transparency activity, and do not bypass TLS warnings or disable certificate verification. [1, 3, 5]
- Scope note:** This advisory does not recommend a blanket DSC replacement or password reset solely because of this incident. Prioritize evidence-based certificate-chain and trust-store checks.

TECHNICAL & RESPONSE DETAILS

Guidance for infrastructure, application, endpoint and security teams

04 TECHNICAL INFORMATION

Root cause / weakness	P-384 EC private keys with values smaller than 256; weakness in key generation, not in the P-384 algorithm. eMudhra attributes this to a wrap/unwrap step; full root-cause investigation remains open.
Affected CAs	Eight intermediate CA key pairs: six TLS-issuing and two code-signing CAs, in G3B/G3C series.
Related trust anchor	emSign ECC Root CA - G3 (root key not reported compromised; root distrusted to reduce ecosystem risk).
CVE / CVSS	No single incident-specific CVE or independently assigned CVSS rating; HIGH is a 443 Labs advisory-priority classification.
Exploitation status	Recoverability independently verified; no confirmed malicious exploitation identified in sources reviewed as of 23 October 2026.
Indicators (IOCs)	No verified exploitation-specific IP addresses, domains or hashes published in the referenced official disclosures.

05 INCIDENT RESPONSE TIMELINE

- 30 Apr 2025** Affected keys created during eMudhra key-generation ceremony.
- 17 Oct 2026** Researcher alerts browser root programs; Chrome and Firefox block vulnerable TLS intermediates.
- 18 Oct 2026** eMudhra revokes all eight affected intermediate CAs.
- 20–21 Oct 2026** Google, Mozilla and CERT-In publish technical/security advisories.
- 22 Oct 2026** eMudhra announces its decision to exit the global SSL/TLS certificate business; replacement support planned.
- 27 Oct 2026*** Chrome Root Store removal of emSign ECC Root CA - G3 expected to reach general channels.

*Scheduled date announced by Google as of 20 October 2026. [3]

06 VALIDATION CHECKLIST

- Server certificates:** Inspect the full deployed chain and confirm no required service depends on emSign ECC Root CA - G3.
- TLS clients:** Verify browsers, servers, mobile apps, proxies, IoT devices and application runtimes reject compromised CA chains; browser-only checks are insufficient.
- Code-signing:** Review applicable code-signing trust policies, vendor advisories and software provenance verification; investigate suspicious signed binaries.
- Change management:** Coordinate replacement certificates, test affected clients, and preserve strict certificate validation during remediation.

07 PRIMARY SOURCES

- [1] CERT-In • 21 Oct 2026
- [2] eMudhra official incident updates • updated 22 Oct 2026
- [3] Google Chrome & Android security advisory • 20 Oct 2026
- [4] Mozilla Security Blog • 20 Oct 2026
- [5] Cloudflare technical response • 20 Oct 2026
- [6] eMudhra global TLS business exit • 22 Oct 2026

Advisory basis. Based on publicly available information as of 23 October 2026. This is an independent 443 Labs customer awareness advisory, not a notice of compromise of any recipient environment. Severity reflects potential impact where unpatched certificate trust persists. Review applicability with your infrastructure and service providers.