

Flash Update: Intermediate Certificate Authority Key Weaknesses

protiviti®
Global Business Consulting

Table of Contents

1. Flash Update 4
2. Incident timeline 5
3. Technical background 6
4. Affected assets 7
5. Threat and risk assessment 8
6. Recommended mitigations 10
7. Detection and threat hunting 12
8. Regulatory and compliance angle (India) 13
9. Third-party and vendor risk questions 14
10. Open questions and what to watch 15





1. Flash Update

Severity: HIGH (ecosystem trust) · Action window: 0–72 hours

The private keys of eight eMudhra (emSign) intermediate certificate authorities were trivially weak and have been recovered from the public certificates. Anyone holding them could issue browser-trusted TLS certificates for any domain, or sign code that appears legitimate.

- **What happened:** A researcher reported the compromise to the Chrome and Mozilla root programs on 17 Oct 2026. The keys were reportedly tiny integers (for example 4, 56 and 237) rather than 384-bit random values.
- **Current status:** eMudhra has revoked all eight certificates. Chrome, Firefox, Apple and Microsoft have blocked them. Mozilla has removed the emSign ECC Root CA – G3 from NSS, and Chrome plans to do the same.
- **Indian exposure:** eMudhra is India's largest licensed Certifying Authority. Government and PSU properties, including UIDAI and the Income Tax e-filing portal, use eMudhra certificates or technology. There is currently no indication that eMudhra's root keys are compromised.
- **Residual risk:** Browsers are protected. Non-browser clients (Go binaries, Python, Java, Node.js, appliances, IoT, embedded trust stores) may still trust these chains until they are updated or rebuilt.
- **Key Action to be taken :** Inventory every emSign-issued certificate and every trust store you operate. Patch non-browser clients now, and plan to move certificates off the emSign G3 hierarchy before the root removals cause outages.



2. Incident timeline

Browsers blocked the TLS intermediates within two hours of the report. Non-browser fixes followed over the next three days. All times are UTC; IST is UTC+5:30.

Date / time (UTC)	Event
21 Oct 2026	eMudhra discloses to the stock exchanges that a flaw during a key-generation event published weak keys for eight intermediate CAs, and rules out a data breach. Public reporting widens in India and globally.
20 Oct 2026	Mozilla (Dennis Jackson) and the Chrome Root Program confirm the compromise publicly. Microsoft blocks the certificates. Mozilla removes emSign ECC Root CA – G3 from NSS 3.131.1. Go 1.27.3 / 1.26.10 ship (CVE-2026-111943). Firefox 158.0.1 and the ESR releases ship (CVE-2026-113470).
19 Oct 2026	Apple blocks the certificates. Other trust stores are notified. Python certifi 2026.10.19 drops the emSign G3 root.
17 Oct 2026, 22:59	Firefox OneCRL block reaches installations with standard settings.
17 Oct 2026, 20:06	Mozilla receives the report.
17 Oct 2026, 19:45	Chrome CRLSet update blocks the six TLS intermediates.
17 Oct 2026, 18:05	Chrome Root Program receives the report from researcher "Wayne", with each key proven by a signed message.
Apr 2025 (reported)	Start of the exposure window, according to researcher Scott Helme.



3. Technical background

The failure was in key generation, not in key storage: the private keys were so small that anyone could derive them from the public certificates.

01

How web trust works.

Browsers and operating systems ship a list of trusted **root CAs**. Roots are kept offline and sign **intermediate CAs**. Intermediates sign the end-entity certificates that websites and software publishers use. A client trusts a certificate if it can build a chain from it, through an intermediate, to a trusted root. Whoever holds an intermediate's private key can therefore issue certificates that clients accept, for any domain the intermediate is not technically restricted from.

02

What went wrong.

The affected intermediates use elliptic-curve (ECC) keys. An ECC private key should be a random 384-bit number, which is far too large to guess. Researchers found that eMudhra's keys were tiny integers such as 4, 56, 66, 115, 155, 156, 230 and 237. With a key that small, the private key can be found from the public key by simply trying small numbers. Scott Helme reports recovering all eight on a laptop in under a second.

03

Why it matters.

This is a systemic process failure. Eight keys failed together, which points to a broken key-generation ceremony, HSM configuration or tooling rather than a single slip. eMudhra describes it as a flaw during a key-generation event. Proper ceremonies use certified hardware security modules with audited randomness and witnesses, and they should catch an out-of-range key.

04

Proof of compromise.

The researcher signed the message "We have a problem here – Wayne" with each of the eight keys and published the signatures, so anyone can verify the compromise with OpenSSL (proof page).



4. Affected assets

Eight intermediates are compromised: six for TLS (websites) and two for code signing. All belong to the emSign G3 (ECC) hierarchy.

Certificate (CN)	Purpose	Issuing entity	Chains to
EM DV TLS CA - G3B	TLS, domain validated	eMudhra BV (Netherlands)	emSign Root TLS CA - G3 → emSign ECC Root CA - G3
EM DV TLS CA - G3C	TLS, domain validated	eMudhra Inc (USA)	emSign Root TLS CA - G3 → emSign ECC Root CA - G3
EM OV TLS CA - G3B	TLS, organization validated	eMudhra BV	emSign Root TLS CA - G3 → emSign ECC Root CA - G3
EM OV TLS CA - G3C	TLS, organization validated	eMudhra Inc	emSign Root TLS CA - G3 → emSign ECC Root CA - G3
EM EV TLS CA - G3B	TLS, extended validation	eMudhra BV	emSign Root TLS CA - G3 → emSign ECC Root CA - G3
EM EV TLS CA - G3C	TLS, extended validation	eMudhra Inc	emSign Root TLS CA - G3 → emSign ECC Root CA - G3
EM OV CS CA - G3B	Code signing	eMudhra BV	emSign G3 hierarchy
EM OV CS CA - G3C	Code signing	eMudhra Inc	emSign G3 hierarchy

Cross-signed copies. Each of the eight also exists as a second certificate with the same public key, cross-signed by Sectigo under the AAA Certificate Services root. Chrome's block matches the public key, so it covers these copies too. Chrome and Firefox stopped trusting AAA Certificate Services for TLS in April 2025, but Apple's iOS 26 / macOS 26 root list still includes it.

Root status.

- **emSign ECC Root CA – G3:** removed from Mozilla NSS on 20 Oct; Chrome will remove it in root store version 43; dropped from certifi, webpki-roots and Homebrew.
- **emSign Root CA – G1:** under review by Chrome. Not reported as compromised.
- **eMudhra's statement:** only one of the eight was used in production, and no end-user certificates were issued from these keys. This has not yet been independently verified.

Full certificate details and SHA-256 hashes are on Mozilla's disclosure page.



5. Threat and risk assessment

Our overall rating is **High**. Likelihood of past abuse is low to moderate, but impact would be severe, and availability risk from root removals is near certain for some organisations.

Risk	Likelihood	Impact	Who is most exposed
Website impersonation / man-in-the-middle via forged TLS certificates	Low for browsers; Medium for non-browser clients	Critical	APIs, mobile apps, Go/Python/ Java/Node services, appliances that skip revocation checks
Malware signed with the code-signing intermediates	Medium	High	Windows and Java endpoints, software supply chains, government desktops
Service outages as clients drop the emSign G3 root	High	Medium–High	Any site or API whose chain ends at emSign ECC Root CA – G3 or AAA Certificate Services
Undetected historical misuse (exposure since ~April 2025)	Unknown	High	Targeted users of high-value Indian portals
Trust and reputational damage to eMudhra-dependent services	High	Medium	Government, PSUs, BFSI, eSign / DSC users

- **Impersonation and MITM.** A forged certificate lets an attacker in a network path (rogue Wi-Fi, compromised ISP or router, DNS hijack) intercept credentials and data while users see a valid padlock. Chrome found no TLS certificates from these intermediates in Certificate Transparency logs before the block, so CT-enforcing browsers are well protected. Clients that do not enforce CT or check revocation remain exposed.
- **Malicious code signing.** The two code-signing keys could make malware look like trusted software. Chrome's TLS block does not cover code signing, so protection depends on OS and platform revocation checks.



- **Exposure window.** Researchers say the keys have been recoverable since about April 2025. Holding a key does not prove fraudulent certificates were issued, and there is no public evidence of attacks. However, there is no reliable way to detect misuse outside CT logs.
- **Sector exposure in India.** eMudhra is India's largest licensed CA. Government portals (including UIDAI and Income Tax e-filing), PSUs, banks and eSign/DSC services depend on its certificates or technology. They face both targeted impersonation risk and outage risk if their chains rely on the removed root.
- **Availability risk.** Removing roots cuts off every legitimate certificate below them, not just the bad ones. Mozilla warns that some servers will become unreachable for non-Firefox users of its trust list until they move to new chains.



6. Recommended mitigations

Prioritise non-browser clients and your own emSign-issued certificates. Browsers are already protected.

Immediate (0–72 hours)

- **Inventory emSign certificates you serve.** Scan public and internal endpoints (for example with your CLM tool, openssl s_client -showcerts, or nmap ssl-cert) for chains containing "emSign", "EM DV/OV/EV TLS CA - G3" or AAA Certificate Services.
- **Inventory trust stores you operate.** Include OS stores, Java cacerts, container base images, language bundles (certifi, Node, Go), proxies, load balancers, WAFs, MDM profiles and appliances.
- **Block the eight intermediates** wherever the software allows per-certificate distrust, using the SHA-256 hashes from Mozilla's disclosure page.
- **Where per-certificate blocking is impossible, remove trust** in emSign ECC Root CA – G3 (and emSign Root TLS CA – G3), as Mozilla advises.
- **Patch and rebuild:** Go 1.27.3 / 1.26.10 (rebuild every binary), certifi 2026.10.19, NSS 3.131.1, webpki-roots 1.0.10, Firefox if Remote Settings is disabled.
- **Confirm browser revocation updates** (Chrome CRLSet, Firefox OneCRL, Windows disallowed list) are not blocked by proxies or policy.
- **Enable revocation checking with hard-fail** in clients that support it.
- **Brief the SOC and stakeholders**, and decide on CERT-In reporting (Section 9).

Short term (1–4 weeks)

- **Reissue certificates** that chain to the emSign G3 hierarchy from another trusted CA, or from a confirmed-unaffected eMudhra hierarchy, before root removals break clients.
- **Generate fresh key pairs** for every reissued certificate; do not reuse private keys.
- **Review code-signed software** in your estate signed under EM OV CS CA – G3B / G3C, and re-sign internal software.
- **Search Certificate Transparency logs** (crt.sh, Censys) for certificates on your domains issued by the affected intermediates.
- **Add CAA DNS records** that list only the CAs you use.
- **Patch Node.js and Composer** when fixes ship; use a custom CA blocklist meanwhile.
- **Test critical integrations** (payment gateways, government APIs, partner B2B links) against updated trust stores.



Strategic (1–6 months)

- **Crypto-agility:** be able to swap a CA, root or algorithm across the estate within days.
- **CA diversification:** keep a pre-approved secondary CA and pre-provisioned backup certificates for critical services.
- **Certificate lifecycle management (CLM):** automated discovery, renewal (ACME) and alerting; prepare for shorter certificate lifetimes.
- **Trust-store hygiene:** a standard, centrally managed trust store per platform, refreshed on a schedule, including container images and appliances.
- **CT monitoring:** continuous alerts for any new certificate issued for your domains.
- **Vendor risk:** add CA and PKI incidents to third-party risk reviews (Section 10).



7. Detection and threat hunting

There is no complete way to detect past misuse. Hunt where certificate data is logged, and treat any hit as a confirmed incident.

Indicators of compromise (IOCs)

- **Issuer names:** EM DV TLS CA - G3B/G3C, EM OV TLS CA - G3B/G3C, EM EV TLS CA - G3B/G3C, EM OV CS CA - G3B/G3C.
- **Public-key and certificate SHA-256 hashes:** take the authoritative list from Mozilla's disclosure page and the Go CVE-2026-111943 patch. Do not retype hashes from secondary sources.

Hunting steps

1. **TLS inspection and proxy logs:** search for server certificates whose issuer matches the IOC names, especially on domains you do not expect to use eMudhra (for example, your own or major cloud and banking domains).
2. **Network sensors (Zeek, Suricata):** query x509.log / TLS metadata for the issuer names and hashes since April 2025.
3. **Certificate Transparency:** query crt.sh or Censys for your domains with these issuers. Note that Chrome found none before the block, but non-CT certificates would not appear.
4. **Endpoint / EDR:** search for executables, drivers, MSI or JAR files whose signer chains to EM OV CS CA – G3B / G3C. Flag any not from a known vendor.
5. **Application logs:** look for unexpected TLS failures after trust-store updates. These show which services still depend on the emSign G3 chain.

Suggested detection rules

- Alert on any TLS session where the issuer is one of the eight intermediates.
- Alert on any newly seen certificate for your domains from an unexpected CA (CT monitoring).
- Alert on code execution of binaries signed under the two code-signing intermediates.

If you find a hit: isolate affected hosts, preserve logs and certificates, rotate credentials that crossed the intercepted channel, and report to CERT-In within six hours.



8. Regulatory and compliance angle (India)

Most organisations do not need to report the eMudhra incident itself. A report is triggered if you find misuse, interception or impact on your own systems. Confirm specific obligations with your legal and compliance teams.

Regulator / framework	Relevance	Suggested action
CERT-In (Directions of April 2022)	Covered incidents, including attacks on PKI and digital certificates, must be reported within 6 hours of noticing them	Report any confirmed misuse, forged certificate or interception; track CERT-In advisories on this incident
Controller of Certifying Authorities (CCA), IT Act 2000	Licenses eMudhra as a CA in India; oversight of CA practices	Watch for CCA directions on eMudhra and on DSC / eSign continuity
RBI (IT governance and cyber security directions)	Banks and NBFCs must manage third-party and cryptographic risk and report incidents	Assess internet banking, UPI and payment-gateway certificate chains; brief the CISO and board risk committee
SEBI CSCRF	Regulated entities must report cyber incidents and manage vendor risk	Review exposure; record the vendor risk event
DPDP Act 2023	Personal data breaches must be notified to the Data Protection Board and affected people	Applies only if interception led to a personal data breach
Sectoral / government (NIC, MeitY, CSIRT units)	Government and PSU properties rely on eMudhra	Coordinate with NIC / sector CSIRT before reissuing certificates on gov.in / nic.in properties

Documentation: keep a dated record of your assessment, the inventory results and the actions taken. This supports audits and shows due diligence even if no incident is found.



9. Third-party and vendor risk questions

Send these to critical suppliers, hosting providers, payment partners and software vendors. Ask for a written response within 5 working days.

1. Do any of your services, APIs or products present certificates issued by eMudhra / emSign, especially the G3 hierarchy?
2. Have you updated trust stores in your products, appliances and containers to block the eight intermediates or remove emSign ECC Root CA – G3?
3. Have you rebuilt Go-based components with Go 1.27.3 / 1.26.10 and updated certifi, NSS and other bundles?
4. Is any software you ship to us signed under EM OV CS CA – G3B or G3C? If so, when will you re-sign it?
5. Have you searched TLS, CT and endpoint logs for the IOCs since April 2025? What did you find?
6. What is your plan and date to move any affected certificates to a new chain?
7. Do you have a secondary CA and a documented process to replace certificates quickly?
8. Who is your point of contact for this incident, and how will you notify us of new findings?

For eMudhra directly (if you are a customer): ask for the root-cause report, confirmation of which hierarchies are unaffected, the reissuance timeline, and evidence for the claim that no end-user certificates were issued.



10. Open questions and what to watch

The root cause and the full exposure are still unknown.

- **Root cause:** how the weak keys were generated and why audits did not catch them. eMudhra must report to the root programs and the CA/Browser Forum.
- **Who else holds the keys:** whether anyone besides the researcher recovered them during the exposure window.
- **eMudhra's claims:** independent confirmation that only one intermediate was in production and that no end-user certificates were issued.
- **Chrome's decision on emSign Root CA – G1:** continued trust, restrictions or removal would sharply raise migration urgency.
- **Other root programs:** whether Apple and Microsoft follow Mozilla in removing emSign roots.
- **Pending patches:** Node.js, Composer, Java distributions and appliance vendors.
- **Indian regulators:** any CERT-In advisory or CCA direction, and continuity guidance for DSC and eSign users.
- **Wider impact:** Mozilla and Chrome checked other CAs and found no similar weak keys, but further research may follow.

Face the Future with Confidence®

This publication has been carefully prepared, but should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the person listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti India Member Private Limited nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this presentation, or for any decision based on it.

© 2026 Protiviti India Member Private Limited

241316_OCTOBER2026

Disclaimer
This flash update reflects public information as of 28 Oct 2026 and may change. Regulatory points are general guidance, not legal advice.