

EOTISEC

NATIONAL SECURITY INTELLIGENCE REPORT FOR BUSINESS

EOTISEC Analytical Division

SECTION 1: REPORT IDENTIFICATION

Report Title	eMudhra Weak Intermediate CA Keys: Contained in Browsers, Open in the Long Tail
Report Number	EOTISEC-2026-064
Date of Report	October 23, 2026
Classification	BUSINESS SENSITIVE // EOTISEC SUBSCRIBER DISTRIBUTION
Originator	EOTISEC Analytical Division
Subject	How much risk the eight computable eMudhra intermediate CA keys pose to subscriber organizations over the next six months, how far the contained reading and the long-tail reading each hold up, and what subscribers should do before and after Chrome removes emSign ECC Root CA - G3 on October 27, 2026.
Customer Sector	Higher Education and Research, Technology and Software Development, Financial Services, Healthcare and Medical Devices, Manufacturing and Critical Infrastructure
Prepared By	Sam Liles, PhD, Principal Analyst
Reviewed By	Dr. Samuel Liles, CISO / Principal
Distribution	EOTISEC Subscriber Base

SECTION 2: SCOPE AND PURPOSE

This report assesses the compromise of eight eMudhra intermediate certificate authority (CA) keys that were generated so weakly that anyone can compute them from the public certificates. It answers three questions. How likely is confirmed malicious use within six months? Which client populations stay exposed, and for how long? What disruption will the distrust of emSign ECC Root CA - G3 cause? The source base is open-source reporting collected October 20 through October 23, 2026: root program statements from Google, Mozilla and the Chrome Root Program, government advisories from CERT-In, vendor bulletins from Red Hat and Cloudflare, eMudhra's own statements and exchange filing coverage, independent researcher analysis, and certificate transparency (CT) data reported by CertKit. The report does not cover eMudhra's Indian digital signature and eSign hierarchies, which the company and the Indian government say run on separate infrastructure. It covers other vulnerabilities disclosed the same week only as a brief contrast with PHP2Shell.

SECTION 3: KEY JUDGMENTS

Each judgment below is a primary analytical conclusion drawn from the source material. ICD 203 probability language applies throughout. Confidence level and explanation follow each judgment. Business Impact callout follows each judgment.

KEY JUDGMENT 1: We assess it is very unlikely that the weak keys were used to attack users of current, CT-enforcing browsers before or after the October 17 blocks. Chrome and Firefox blocked the six TLS intermediates within hours of the report, and no TLS certificate chaining to them appeared in CT logs before the block.

Confidence: High. *Google, the Chrome Root Program and Mozilla independently describe the same block times and the same CT finding, and the CT enforcement mechanism is well documented. The residual risk sits with browsers that are badly out of date or that have CT enforcement turned off by policy.*

BUSINESS IMPACT: *Browser-only exposure is not where subscribers should spend effort. Higher Education, Financial Services and every other sector should confirm that managed browsers are current and that no enterprise policy disables CT enforcement or CRLSet and OneCRL updates, then move resources to the non-browser clients in Key Judgment 2.*

KEY JUDGMENT 2: We assess that a residual population of non-browser clients will almost certainly keep trusting the compromised chain through at least mid-2027. Most of these clients read a CA bundle from disk, skip revocation and do not enforce CT, and some embedded devices will trust the chain until the intermediates expire in July 2039.

Confidence: High. *Researcher testing, the community patch tracker, Red Hat, Endor Labs and the CPython release notes all show the same pattern of bundle-by-bundle remediation, with Red Hat Enterprise Linux still unpatched as of October 23. The mechanism is well understood. What is not known is the size of the residual population.*

BUSINESS IMPACT: *Technology and Software Development, Financial Services, Healthcare and Manufacturing subscribers carry most of this exposure through CI/CD runners, container images, language runtimes, server-to-server API clients, appliances and devices with frozen bundles. Inventory every trust store, not only the operating system store, rebuild container images, and segment devices that cannot be updated.*

KEY JUDGMENT 3: We assess it is unlikely that confirmed malicious use of the keys, meaning a forged TLS certificate or a signed binary observed against a real target, will be publicly reported in the next six months.

Confidence: Low. *No source reports misuse, but the absence of reports is weak evidence because offline forgeries used against non-CT clients leave no public trace. A working public forgery tool exists, and the judgment rests mainly on inference about attacker incentives and detection rather than on direct observation.*

BUSINESS IMPACT: *Subscribers should not read the quiet so far as proof of safety. Financial Services and Technology subscribers with high-value API traffic and update channels should treat any network path that a capable adversary could intercept as at risk until clients are patched. Healthcare and Manufacturing subscribers should add the two eMudhra code-signing intermediates to allow-list and EDR rules so that a signed binary would be caught if one appears.*

KEY JUDGMENT 4: We assess it is very likely that some US higher education services will present certificate errors in Chrome after the October 27 root removal, with the disruption caused by the fix rather than by any attacker.

Confidence: Moderate. *CT counts from October 21 show more than 5,000 certificates still on the distrusted chain at 43 of 57 large universities, and Cloudflare-fronted sites at one university already returned errors on October 20. No newer count was available, and replacement pace was high, so the scale on October 27 is uncertain.*

BUSINESS IMPACT: *Higher Education subscribers should finish replacing every certificate whose issuer ends in G3C before October 27 and check load balancers, proxies and appliances that ACME never touches. Every other sector should identify research, grant, identity federation and SaaS partners that use InCommon certificates and expect transient TLS failures on those connections next week.*

KEY JUDGMENT 5: We assess it is likely that organizations that reissued certificates on eMudhra's G1 RSA hierarchy will have to migrate again within twelve months.

Confidence: Moderate. *eMudhra has announced its exit from global TLS, Chrome has said it is evaluating eMudhra's remaining CA certificates, and eMudhra now offers Sectigo certificates to all customers. No root program has ruled on G1, so the timing of a forced move rests on inference.*

BUSINESS IMPACT: *Higher Education subscribers that moved to G1 this week should plan a second migration now and prefer a CA outside eMudhra for new issuance. All sectors should remove CAA records that authorize only emsign.com and confirm that certificate automation can switch CAs without touching each server by hand.*

SECTION 4: SITUATION AND BACKGROUND

Technical Background

On April 30, 2025, eMudhra held a key generation ceremony that created eight intermediate CAs under its emSign ECC Root CA - G3 hierarchy.¹ Six issue TLS certificates at the domain, organization and extended validation levels, in two generations labeled G3B and G3C. The other two issue code-signing certificates. Sectigo cross-signed all eight under its AAA Certificate Services root in May 2025.²

The private keys sit on the NIST P-384 curve, where a private key should be a random 384-bit number. Each of the eight is a whole number below 256. One is the number 4. Researcher Scott Helme recovered all eight from the public certificates in under a second on a laptop.³ The open-source interception proxy mitmproxy merged an option on October 21 that embeds the key for EM OV TLS CA - G3C, labeled d=4, and signs certificates for any host with it.⁴

eMudhra says a key wrap and unwrap step in the ceremony produced a second, weak set of keys alongside the intended strong keys, and that the weak set was published to browser root stores. It has not confirmed the exact root cause.⁵ The weak keys were used operationally. When CRL signatures for six of the intermediates failed in June 2025, eMudhra re-signed the CRLs with the weak keys, and Chrome said that disclosure raised serious concerns about eMudhra's transparency.^{6,7}

A researcher identified only as Wayne found the keys by running Google's open-source paranoid_crypto library against the Common CA Database (CCADB) corpus. A later sweep of all CCADB certificates found no further hits.⁷ Google says it checked every key in its root stores and found no other instance of the failure.⁸

Root Program Response

The Chrome Root Program received the report at 18:05 UTC on October 17 and blocked the six TLS intermediates by public key through a CRLSet update at 19:45 UTC. Mozilla received the report at 20:06 UTC and pushed a OneCRL block that reached Firefox users with standard settings by 22:59 UTC.^{9,10} Apple blocked the intermediates on October 19 and Microsoft on October 20.¹¹ Android devices received an equivalent block through Google Play Services on October 19.⁸

No TLS certificate chaining to the six intermediates was logged to CT before Chrome's block, so no forged certificate from them could have been trusted by default in Chrome or other CT-enforcing clients.⁹⁸ Mozilla removed emSign ECC Root CA - G3 from NSS 3.131.1 on October 20. Chrome's removal of the same root reaches all devices that rely on the Chrome Root Store on the morning of October 27, 2026, Pacific time.¹⁰⁸ Chrome also says it is evaluating whether eMudhra's remaining CA certificates should stay in its store.⁹

The dates in eMudhra's account do not line up with the root programs. eMudhra says it learned of the issue late on October 18, India time, and revoked the eight intermediates on October 19.⁵ CERT-In's advisory gives the revocation date as October 18.¹²

Non-Browser Exposure

Most TLS clients outside browsers trust a CA bundle on disk, do not check revocation by default and do not enforce CT. Helme forged a certificate for api.stripe.com in a local test. curl, Python and Node accepted it with default settings on every Linux and macOS machine he tried, and Windows CryptoAPI accepted it unless revocation checking was on. The intermediates do not expire until July 2039.³

Remediation is moving bundle by bundle. Go, Node.js, Java, Python certifi, pip, uv, Rust webpki-roots, curl's bundle and most Linux distributions shipped fixes between October 19 and October 21.¹¹² CPython shipped expedited releases 3.15.1, 3.14.9 and 3.13.17 on October 23.¹³ As of October 23, the community patch tracker still lists Bottlerocket, Erlang certifi, Composer ca-bundle and Godot as pending, and notes that the curl, git and python3 built into macOS still read an unmodified certificate file.¹¹ Red Hat rates the issue Important across Red Hat Enterprise Linux 6 through 10 and products built on them, and its bulletin revision of October 23 lists no fixed packages, only workarounds.¹⁴ Endor Labs found 25 widely used packages that trust a root in the compromised chains, of which 11 were patched, including a Ruby HTTP library whose bundled roots date to 2015.¹⁵

Red Hat states the attack conditions plainly: the client must trust the chain, the attacker must hold a key, and the attacker must be in a position to intercept TLS.¹⁴ The keys are public, so network position is the only real barrier.

No source reports malicious use. CERT-In says the public disclosures do not establish confirmed exploitation as of October 21.¹² Cloudflare's security review found no active exploitation on its services, and Endor Labs reports none observed.^{16,15} Jackson's site and Mozilla both say whether anyone exploited the flaw before disclosure is unknown.¹¹¹⁰

Collateral Impact

Chrome counted about 30,800 unexpired certificates under emSign ECC Root CA - G3 as of October 21. Of those, 99.9 percent were issued through InCommon, the certificate service Internet2 runs for US higher education, which moved onto eMudhra's CertiNext platform between April and July 2026.⁶ eMudhra estimated that about 30,000 certificates need to move and that about 97 percent were issued through ACME.⁶

On the evening of October 21, CertKit's CT search found 43 of 57 large universities still holding current certificates on the ECC chain, 5,042 in all. RSA issuance at those schools rose from about 600 a day to 3,660 on October 21. Of 1,023 replacements CertKit observed over seven hours, 967 went to eMudhra's RSA chain and 56 to Let's Encrypt.¹⁷ The University of Michigan reported HTTP 526 errors on October 20 after Cloudflare stopped trusting the root for origin connections, and it lists Let's Encrypt as its main alternative because eMudhra's RSA certificates "may not be permanent."¹⁸

Corporate and Government Response

eMudhra's board voted on October 22 to withdraw from the global SSL/TLS certificate business. The company says the business is about 1 percent of revenue, cites rising compliance costs and free competitors, and says "social media amplification" brought scrutiny out of proportion to the business. It says its G1 RSA roots will serve customers until the transition is complete and that it will deliver a full root-cause report to the root programs.¹⁹ A statement update the same day offers Sectigo certificates to all customers as an alternate option.⁵ eMudhra shares hit the 20 percent lower circuit on the BSE on October 21.²⁰

India's Ministry of Electronics and Information Technology formed a team to investigate, and CERT-In issued advisory CIAD-2026-0050 on October 21 and updated it on October 23.²¹² The Internet Freedom Foundation wrote to eMudhra, CERT-In and the ministry on October 21 asking for a complete incident report, an independent audit and a statutory inquiry. It noted that the public cannot see when eMudhra reported to CERT-In.²¹

Concurrent Disclosure for Context

PHP2Shell (CVE-2026-109618 and CVE-2026-109619, CVSS 4.0 score 9.2) was disclosed the same week. As of October 22, watchTowr reported exploitation attempts against its honeypots but no confirmed compromise of victim systems, and the flaws were not on CISA's Known Exploited Vulnerabilities list.²² This report addresses PHP2Shell only as a contrast in Section 5.

SECTION 5: ANALYSIS

Weighing the Contained and Long-Tail Readings

The contained reading rests on strong evidence. Browsers were protected before the public knew, CT shows no certificates issued under the six TLS intermediates before the block, and no source reports misuse. eMudhra's exit removes the CA from future issuance.

The long-tail reading rests on equally strong evidence of a different kind. The keys are public and trivial to use, a mainstream interception tool now ships one of them, and the clients that matter most to an attacker (build systems, update channels, API clients and devices) are the ones that remediate slowest. The question is not whether exposure exists. It does. The question is whether anyone with a network position will use it and whether anyone would see it if they did.

Coverage of PHP2Shell and the eMudhra keys has run in opposite directions. PHP2Shell drew alarm first and is now drawing correction, because exploitation depends on build-specific conditions. The eMudhra keys drew ridicule and little alarm, yet exploiting them takes no skill once an attacker can intercept traffic. In both cases press attention tracked visible disruption rather than exploitability. Subscribers should weight their response to the eMudhra keys by exploitability and network exposure, not by the volume of coverage.

Assumptions

Assumption 1: The eight eMudhra keys are the only weak CA keys in the public WebPKI. Google's check of every key in its root stores and an independent sweep of the CCADB support this. It fails if another CA key with low entropy is found, which would widen every judgment in this report beyond one hierarchy.

Assumption 2: CT enforcement in Chrome, Safari and Firefox worked as the root programs describe, and no forged certificate was trusted by those browsers. Consistent statements from Google, Mozilla and the Chrome Root Program support this. It fails if a CT log operator or a browser enforcement bug is found to have admitted an unlogged certificate.

Assumption 3: Network position remains the binding constraint on exploitation. Red Hat's stated conditions support this. It fails if a widely deployed client fetches code or credentials over a path that an attacker can redirect at scale, for example through DNS hijacking, BGP misdirection or a compromised network appliance.

Assumption 4: Enterprise Linux vendors and major language ecosystems will ship trust store fixes within weeks. The pace of fixes from October 19 to October 23 supports this. It fails if Red Hat errata slip past mid-November, which would extend exposure across a large share of server and container infrastructure.

Assumption 5: Malicious use, if it occurs against an organization that monitors its traffic, would eventually be detected and disclosed. This is the weakest assumption. Offline forgeries leave no CT trace, so detection depends on the victim noticing an unexpected issuer.

LINCHPIN ASSUMPTION: Assumption 3 is the linchpin. Key Judgment 3 depends on the premise that exploitation requires a targeted network position, which limits use to capable actors against chosen targets. If a path exists to intercept a widely used update or package channel at scale, a single operation could reach many unpatched clients, and the probability of confirmed malicious use would rise sharply. Evidence that would break it includes a report of DNS or BGP manipulation against a software distribution domain during the exposure window, or a forged certificate observed on a shared network appliance. This assumption should be revisited at each production cycle.

Analysis of Alternatives

For Key Judgment 1, the primary alternative is that a forged certificate was trusted by a browser through a gap in CT enforcement, such as an enterprise policy that disables it. We assess this alternative as very unlikely because the root programs report no logged certificates and enterprise CT exemptions are rare and visible to administrators.

For Key Judgment 2, the primary alternative is that the residual population shrinks to a negligible level by early 2027 as distributions, runtimes and base images update. We assess this alternative as unlikely because embedded devices, vendored bundles such as the 2015-era Ruby library bundle, and unmaintained containers do not follow vendor update cycles.

For Key Judgment 3, the primary alternative is that a capable actor has already used, or will use, the keys and that the use becomes public. We assess this alternative as unlikely because exploitation requires a network position against each target, the browser path is closed, and offline forgeries against non-CT clients are hard to detect even when they occur. A public tool lowers the skill barrier but not the access barrier.

For Key Judgment 4, the primary alternative is that universities finish replacement before October 27 and disruption stays negligible. We assess this alternative as unlikely because about 5,000 certificates remained on the chain four business days before the deadline and appliances outside ACME automation require manual work.

For Key Judgment 5, the primary alternative is that Chrome and Mozilla keep eMudhra's G1 root trusted long enough for G1 certificates to expire naturally. We assess this alternative as unlikely because eMudhra itself is exiting, Chrome has an open evaluation, and the June 2025 CRL handling and the October 14 G1 CRL signature failure give root programs grounds to act.

Implications by Customer Sector

Higher Education and Research: This sector carries nearly all of the collateral cost. Replace every certificate on the InCommon OVG3C and DVG3C intermediates before October 27, including on load balancers, proxies and appliances. Treat G1 RSA reissuance as temporary and plan a move to a CA outside eMudhra. Check Cloudflare origin settings, since Cloudflare already distrusts the root for origin connections.

Technology and Software Development: CI/CD runners, container base images, vendored CA bundles and curl-to-shell installers are the highest-value targets for a forged certificate. Rebuild images with layer caching disabled, update Go and rebuild binaries, update Node, Java, Python, pip and uv, and search repositories for bundled PEM files. Software publishers should confirm that no release pipeline trusts the eMudhra code-signing intermediates.

Financial Services: Server-to-server API calls, payment integrations and OAuth token exchanges often run on runtimes with their own CA bundles. Confirm the trust store each service actually uses rather than relying on host patching. Enable revocation checking or certificate pinning on high-value outbound connections where the client supports it.

Healthcare and Medical Devices: Connected medical devices and clinical appliances often ship frozen trust stores and cannot be patched on short notice. Identify devices that trust emSign ECC Root CA - G3 or Sectigo AAA Certificate Services, request vendor guidance, and segment devices that cannot be updated so that an attacker cannot reach their update or telemetry paths.

Manufacturing and Critical Infrastructure: OT gateways, embedded controllers and appliances that phone home for updates face the longest exposure, potentially until 2039. Inventory devices with TLS-based update or command channels, restrict their egress to known destinations, and monitor for unexpected certificate issuers on those flows.

Changes from Prior Assessment

No prior EOTISEC assessment exists on this topic. This report establishes the baseline. The analyst maintains a daily tracker with indicator tables for both the contained and long-tail readings, and future updates will report changes against the October 23, 2026 baseline, with particular attention to Chrome's decision on G1, Red Hat errata and any report of malicious use.

SECTION 6: INFORMATION GAPS AND COLLECTION REQUIREMENTS

For each gap, the format is: Gap statement. Analytical significance. Collection requirement.

1. Gap: No mechanism exists to detect past or present use of forged certificates against clients that do not enforce CT.

Analytical significance: Key Judgment 3 is most sensitive. Any confirmed sighting would move the judgment toward likely and change the report's overall balance.

Collection requirement: Monitor vendor threat intelligence, incident response disclosures, VirusTotal and EDR telemetry for certificates or binaries chaining to the eight intermediates, and the Mozilla dev-security-policy list.

2. Gap: The size of the residual non-browser population is unknown. Mozilla's Dennis Jackson published user-agent statistics from his test site on October 21, but the data page was not reachable during collection.

Analytical significance: Key Judgment 2 is most sensitive. Data showing rapid decline would support a shorter exposure window.

Collection requirement: Retrieve the test-site statistics, track Red Hat errata, and track remaining pending entries on the community patch tracker.

3. Gap: Chrome has not ruled on eMudhra's G1 root, and eMudhra has not answered Chrome's questions publicly.

Analytical significance: Key Judgment 5 is most sensitive. A distrust decision would raise it to very likely. Retention would lower it.

Collection requirement: Monitor the CCADB public list, Mozilla bug 2083449 and eMudhra statements.

4. Gap: No InCommon migration count after the evening of October 21 was available.

Analytical significance: Key Judgment 4 is most sensitive. A count near zero by October 26 would lower it.

Collection requirement: Query CT logs for unexpired certificates under InCommon OVG3C and DVG3C, and monitor university IT status pages on October 27 and 28.

5. Gap: eMudhra's root cause report has not been published, and the mitigating account of key generation is disputed on the Mozilla list.

Analytical significance: Assumption 1 and Key Judgment 5 are most sensitive. A cause outside the one ceremony could implicate other hierarchies.

Collection requirement: Monitor Mozilla bug 2083449, eMudhra's statement page, and any MeitY or CERT-In findings.

SECTION 7: SOURCE SUMMARY STATEMENT

This report uses only open-source material. No classified sources were used. Primary sources include root program statements (the Chrome Root Program post to the Mozilla dev-security-policy list, Google's security blog and the Mozilla Security Blog), a government advisory (CERT-In CIAD-2026-0050), vendor bulletins (Red Hat RHSB-2026-012 and Cloudflare), the community patch tracker maintained by Mozilla engineer Dennis Jackson, the mitmproxy source commit, and eMudhra's own statement page and press release. Secondary sources include The Hacker News, CertKit, Scott Helme, Endor Labs, Business Standard, SecurityOnline, watchTower, the University of Michigan and the Internet Freedom Foundation.

eMudhra's statements are first-party corporate communications from the party at fault and carry advocacy risk. They were used for eMudhra's own account and actions and were checked against root program statements where possible. Endor Labs, CertKit and Cloudflare are vendors with commercial interests in certificate and supply chain tooling.

Single-source dependencies: the university CT counts and replacement figures in Key Judgment 4 come from CertKit alone. The key values come from Helme, with the value 4 independently confirmed by the mitmproxy commit. Chrome's count of about 30,800 certificates and its questions to eMudhra come from Mozilla bug 2083449, which could not be opened from the collection environment, so they are cited through The Hacker News and CertKit. The Endor Labs package counts come from that vendor alone.

SECTION 8: ICD 503 CONSIDERATIONS AND ATT&CK / D3FEND MAPPING

ICD 503 considerations apply because the compromised keys undermine the authentication layer that information systems rely on to verify remote services and software. A forged certificate lets an attacker impersonate any server to a client that still trusts the chain, which defeats confidentiality and integrity protections on data in transit and on software delivered over TLS.

Risk to Information Systems and Data: Systems at risk are TLS clients that rely on static CA bundles, including CI/CD pipelines, container workloads, language runtimes, API clients, package managers, self-updating software, network appliances, and IoT, OT and medical devices. Data flows at risk include API credentials, OAuth tokens, payment data, software updates and telemetry. Windows systems that miss automatic trust list updates face a separate code-signing risk.

NIST RMF Alignment: The Monitor phase is implicated first, since organizations must detect untrusted issuers and confirm trust store changes. The Implement and Assess phases are implicated for control SC-17 (Public Key Infrastructure Certificates) and SC-8 (Transmission Confidentiality and Integrity). System security plans should document every trust store each system uses, including bundled ones, and the process and time to update them.

Supply Chain Risk: The exposure flows through software suppliers who bundle trust stores into libraries, runtimes, images and firmware. Organizations following NIST SP 800-161 and the Secure Software Development Framework should ask suppliers which CA bundle their products use and when they removed the compromised roots, and should treat certificate trust as part of software bill of materials review.

ATT&CK Technique Mapping

Technique ID	Technique Name	Tactic	Application to This Report	Status
T1588.004	Obtain Capabilities: Digital Certificates	Resource Development	The private keys are computable from public certificates and one is published in mitmproxy. Any actor can obtain signing capability under a publicly trusted chain without stealing anything.	ASSESSED
T1587.003	Develop Capabilities: Digital Certificates	Resource Development	An actor can mint leaf certificates for any domain under the six TLS intermediates, as Helme demonstrated for api.stripe.com in a lab.	ASSESSED

Technique ID	Technique Name	Tactic	Application to This Report	Status
T1557	Adversary-in-the-Middle	Credential Access, Collection	A forged certificate lets an actor with a network position intercept and modify TLS traffic from clients that trust the chain, including API calls and token exchanges.	ASSESSED
T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	Initial Access	Clients that download installers, packages or updates over TLS without separate signature checks could be served attacker code through a forged certificate.	ASSESSED
T1553.002	Subvert Trust Controls: Code Signing	Defense Evasion	The two code-signing intermediates chain to a root that Windows trusts directly. Binaries signed with them appear legitimately signed to systems that skip revocation.	ASSESSED
T1573.002	Encrypted Channel: Asymmetric Cryptography	Command and Control	An actor could present a forged certificate for a legitimate domain on command-and-control infrastructure to blend with expected traffic on unpatched clients.	ASSESSED

All mappings are *ASSESSED*. No source reports confirmed adversary use of the keys, so no technique is marked *REPORTED*. The *mitmproxy* option is a published capability, not an observed attack.

D3FEND Countermeasure Mapping

D3FEND Technique	D3FEND ID	Addresses ATT&CK	Application and Priority
Software Update	D3-SU	T1557, T1195.002	Update operating system trust stores, language runtimes, CA bundles and container base images, and rebuild Go binaries. HIGH priority because static bundles are the exposed population in Key Judgment 2 and Red Hat errata are still pending.
Software Inventory	D3-SWI	T1557, T1195.002	Inventory every trust store in use, including vendored PEM files, SDK root lists and firmware bundles. HIGH priority because Endor Labs found trust stores in packages that host patching does not reach.
Active Certificate Analysis	D3-ACA	T1557, T1573.002	Test each client path against the community test hosts to confirm it rejects the compromised chain. MODERATE priority because browser tests do not prove that background services are protected.
Passive Certificate Analysis	D3-PCA	T1557, T1573.002	Alert on TLS sessions presenting any of the eight intermediates or their Sectigo cross-signs on monitored egress. MODERATE priority because offline forgeries leave no CT trace and network observation is one of few detection paths.
Executable Denylisting	D3-EDL	T1553.002	Block binaries signed by EM OV CS CA - G3B or G3C and confirm the 16 certificates sit in the Windows Disallowed store on machines that miss automatic updates. MODERATE priority because Microsoft has blocked them for updated systems.
Certificate Pinning	D3-CP	T1557, T1195.002	Pin issuers or keys on high-value outbound connections and update channels where the client supports it. LOW TO MODERATE priority because pinning carries operational cost and only some clients support it.

Priority designations reflect the exposure described in this report: unpatched static trust stores and the absence of CT-based detection for non-browser clients. They are not generic best-practice ratings.

SECTION 9: ANALYTIC TRADECRAFT SELF-CERTIFICATION

ICD 203 Requirement	Status	Notes
Objectivity: The analysis is free of advocacy, personal preference, or policy bias.	CONFIRMED	The report weighs the contained and long-tail readings against each other and assigns judgments on both sides. It treats eMudhra's statements as first-party claims and tests them against root program statements.
Independence of Political Consideration: No judgment was shaped to support a particular outcome or audience preference.	CONFIRMED	Judgments follow the evidence on browser protection and on non-browser exposure regardless of how either reflects on eMudhra, Indian regulators or the root programs.

ICD 203 Requirement	Status	Notes
Timeliness: Source material is current and the report addresses matters actionable by the customer.	CONFIRMED	<i>Sources run through October 23, 2026, ahead of the October 27 Chrome root removal that drives the most time-sensitive actions.</i>
Based on All Available Sources: All source material provided was considered. Gaps are documented in Section 6.	CONFIRMED	<i>Root program, government, vendor, researcher and corporate sources were reviewed. Bug 2083449 and Jackson's user-agent statistics could not be reached and are listed as gaps.</i>
Source Credibility Described: Source quality is addressed in Section 7.	CONFIRMED	<i>Section 7 identifies first-party corporate sources, vendor sources and single-source dependencies, including the CertKit counts.</i>
Uncertainty Expressed: Probability and confidence language conforms to ICD 203 standards.	CONFIRMED	<i>Each judgment uses one ICD 203 probability term and a separate confidence level with rationale. Key Judgment 3 carries Low confidence because detection limits the evidence.</i>
Assumptions Distinguished from Facts: All assumptions are labeled. Linchpin assumptions are identified.	CONFIRMED	<i>Section 4 holds facts only. Five assumptions are stated with failure conditions, and network position as the binding constraint is the linchpin.</i>
Alternatives Incorporated: At least one alternative hypothesis is addressed for each major judgment.	CONFIRMED	<i>Section 5 assesses one alternative for each of the five judgments with ICD 203 language.</i>
Customer Relevance Addressed: Implications for the relevant stakeholder are stated specifically.	CONFIRMED	<i>Five sectors receive specific actions tied to their trust store and certificate exposure.</i>
Clear and Logical Argumentation: The main analytic message is stated up front in Section 3.	CONFIRMED	<i>Section 3 states the split up front: browsers contained, non-browser clients exposed, malicious use unproven and hard to detect, and collateral disruption likely.</i>
ATT&CK and D3FEND Mapping Completed: REPORTED and ASSESSED attributions are correctly distinguished. Priority designations are grounded in the specific incident.	CONFIRMED	<i>All techniques are marked ASSESSED because no adversary use is reported. Countermeasure priorities are tied to the pending Red Hat errata, bundled trust stores and the CT detection gap.</i>

SECTION 10: ENDNOTES

1 eMudhra Limited. "eMudhra Statement on Recent Certificate Security Incident," Update 3. eMudhra, October 21, 2026. <https://emudhra.com/en/post/certificate-security-incident>

2 Khandelwal, Swati. "Eight eMudhra CA Keys Compromised, Triggering Emergency Fixes Across Browsers and Software." The Hacker News, October 20, 2026, updated October 21, 2026. <https://thehackernews.com/2026/10/eight-emudhra-ca-keys-compromised.html>

3 Helme, Scott. "Eight Bits of Trust: eMudhra's CA keys cracked in milliseconds." scotthelme.co.uk, October 20, 2026. <https://scotthelme.co.uk/eight-bits-of-trust-emudhras-ca-keys-cracked-in-milliseconds/>

4 mitmproxy project. "Add --emudhra option (#8500)," commit 1692344. GitHub, October 21, 2026. <https://github.com/mitmproxy/mitmproxy/commit/169234499088fc2c414644a67efaed3d64ae2e3b>

5 eMudhra Limited. "eMudhra Statement on Recent Certificate Security Incident," Updates 2 through 4. eMudhra, October 20 to 22, 2026. <https://emudhra.com/en/post/certificate-security-incident>

6 Khandelwal, Swati. "eMudhra to Exit Global SSL/TLS Business After 8 Intermediate CA Keys Found Easily Guessable." The Hacker News, October 22, 2026. Cites Mozilla bug 2083449 comments 11, 19 and 30. <https://thehackernews.com/2026/10/emudhra-to-exit-global-ssl-tls-business.html>

7 Mozilla dev-security-policy list. "Compromised eMudhra Intermediate Certificates," posts by Wayne (October 21, 2026), Andrew Ayer (October 22, 2026) and others. <https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/0R3XLJL6FuE>

8 Chrome and Android Security Teams. "Protecting Chrome and Android Users from Compromised eMudhra Intermediate CA Certificates." Google, October 20, 2026. <https://blog.google/security/protecting-chrome-and-android-users-from-compromised-emudhra-intermediate-ca-certificates/>

9 Chrome Root Program. Post to Mozilla dev-security-policy list, "Compromised eMudhra Intermediate Certificates," October 20, 2026. <https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/0R3XLJL6FuE/m/Kp1v6CPuAAAJ>

10 Mozilla. "Protecting Firefox users following the compromise of eMudhra intermediate certificates." Mozilla Security Blog, October 20, 2026, updated October 21, 2026. <https://blog.mozilla.org/security/2026/10/20/protecting-firefox-users-following-the-compromise-of-emudhra-intermediate-certificates/>

- 11 Jackson, Dennis, and contributors. "eMudhra Intermediate CA Compromise." October 20, 2026, patch tables as viewed October 23, 2026. <https://emudhra.we-have-a-problem.com/>
- 12 CERT-In. "Compromise of eMudhra Intermediate CA Certificates," Advisory CIAD-2026-0050. October 21, 2026, updated October 23, 2026. <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2026-0050>
- 13 "Python Ships Emergency Releases After emSign CA Certificate Incident." SecurityOnline, October 23, 2026. Primary python.org release notes not independently opened. <https://securityonline.info/python-emsign-ca-certificate/>
- 14 Red Hat. "RHSB-2026-012 Certificate compromise - eMudhra (CVE-2026-111943)." Red Hat Customer Portal, October 21, 2026, revision of October 23, 2026, 02:10. <https://access.redhat.com/security/vulnerabilities/RHSB-2026-012>
- 15 Endor Labs. "eMudhra Intermediate CA Compromise: The Trust Stores You Patched and the Ones You Didn't Know You Had." October 21, 2026, updated October 23, 2026. <https://www.endorlabs.com/learn/emudhra-intermediate-ca-compromise-the-trust-stores-you-patched-and-the-ones-you-didnt-know-you-had>
- 16 Patton, Christopher, Bas Westerbaan, Trishna, and Jeremy Hartman. "8 eMudhra certificates are compromised. Here's what you need to know." Cloudflare Blog, October 20, 2026. <https://blog.cloudflare.com/emudhra-certificate-compromise>
- 17 Gardner, Todd H. "Internet2's certificate authority (eMudhra) is being distrusted." CertKit, October 22, 2026. <https://www.certkit.io/blog/emudhra-internet2-incommon-distrust>
- 18 University of Michigan Safe Computing. "Root Certificate Authorities Distrusted." October 20, 2026. <https://safecomputing.umich.edu/security-alerts/root-certificate-authorities-distrusted>
- 19 eMudhra Limited. "eMudhra to Exit global SSL/TLS Certificate Business." Press release, October 22, 2026. <https://emudhra.com/en/press-release/emudhra-to-exit-global-ssl-tls-certificate-business>
- 20 "eMudhra tanks 20%: Why IT-enabled services stock sank in Wednesday's trade." Business Standard, October 21, 2026. https://www.business-standard.com/markets/news/emudhra-tanks-20-why-it-enabled-services-stock-sank-in-wednesday-s-trade-126102100353_1.html
- 21 Internet Freedom Foundation. "A private key with the value 4: IFF writes to eMudhra, CERT-In and MeitY on the compromise of eMudhra's certificate authority keys." October 21, 2026. <https://internetfreedom.in/a-private-key-with-the-value-4-iff-writes-to-emudhra-cert-in-and-meity-on-the-compromise-of-emudhras-certificate-authority-keys/>
- 22 watchTowr. "Frequently Asked Questions About PHP Remote Code Execution (PHP2Shell CVE-2026-109618 and CVE-2026-109619)." Updated October 22, 2026. <https://watchtowr.com/intelligence/php-cve-2026-109618-faq/>