



National Cyber Emergency Response Team

Government of Pakistan



NCA-20.211026 – National CERT Advisory

Critical eMudhra (emSign) Certificate Authority Key Compromise: Emergency Trust-Store Updates Required

It has been observed, as of 21 October 2026, the confirmed compromise of eight intermediate Certificate Authority (CA) private keys operated by eMudhra (emSign): six issuing TLS certificates and two used for code signing. The affected ECDSA P-384 keys were generated with insufficient entropy and were independently recovered by Mozilla within hours of the report, creating a genuine certificate-forgery risk for applications and devices that still trust the affected certificate chains.

Emergency protections have been deployed across major browsers and operating systems, and security updates are available for numerous developer platforms and trust stores. No malicious exploitation has been publicly established. eMudhra reports that the affected intermediates issued no legitimate end-entity certificates, and Google reports that no TLS certificates chaining to the six TLS intermediates appeared in Certificate Transparency (CT) logs before it blocked them. This substantially limits exposure for CT-enforcing browsers but does not eliminate risk for non-browser applications that neither enforce CT nor reliably reject revoked certificates. This advisory suggests organizations to update trust stores, distrust the compromised intermediates, and identify applications that maintain independent certificate stores.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-20.211026
Threat Type	Certificate Authority Key Compromise / Certificate Forgery and Man-in-the-Middle (MITM)
Severity	Critical
Attack Vector	Network – forged certificates signed with recovered CA private keys, presented through traffic interception or redirection
Authentication Required	None
User Interaction	Not required beyond the client connecting to an attacker-controlled or intercepted endpoint
Risk Rating	Critical (Confidentiality & Integrity Impact)
Scope & Applicability	Federal & Provincial Government entities, Critical Information Infrastructure (CII), Financial Institutions, and all organizations operating clients, servers, devices, or applications that trust emSign/eMudhra certificate chains

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



IMPACT ANALYSIS

Failure to apply the required trust-store protections may result in:

1. **TLS Certificate Forgery:** Attackers can sign fraudulent certificates for domains they do not control.
2. **Man-in-the-Middle Interception:** Reading or manipulating HTTPS communications on clients that accept forged chains.
3. **Service Impersonation:** Fraudulent but apparently trusted websites, APIs, and services.
4. **Code-Signing Trust Abuse:** Two compromised intermediates were used for code signing, which may undermine signature trust.
5. **Non-Browser Application Exposure:** Clients that neither enforce Certificate Transparency nor reliably reject revoked certificates remain at risk.
6. **Independent Trust-Store Gaps:** Java, Python, Node.js, statically compiled Go binaries, containers, and embedded systems are not secured by browser updates.
7. **Incomplete Remediation:** Each key also has a Sectigo cross-signed certificate (16 certificate instances), so alternative trust paths may remain.
8. **Service Disruption:** Sites relying on emSign ECC Root CA - G3 may fail once Google removes it from the Chrome Root Store (expected 27 October 2026).

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Cryptographic Key-Generation Weakness / Certificate Authority Compromise
Threat Status	Disclosed 17 October 2026; exploitation not confirmed; vendor protections deployed, patching in progress
Root Cause	Faulty key generation during a key wrap/unwrap operation produced low-entropy ECDSA P-384 private keys; eMudhra reports no infrastructure breach and its investigation is ongoing
Target Scope	Government, CII, Financial Sector, Enterprises, Developers, Device and Appliance Vendors, Individual Users
Attack Complexity	Requires the attacker to intercept or redirect the connection of a client that still trusts the affected chain
Privileges Required	None
Affected Systems	Eight intermediate CAs (6 TLS, 2 code signing; 16 certificate instances including Sectigo cross-signs) and any browser, OS, runtime, library, container, or device trusting them

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



Characteristic	Details
Reference Classifications	CVE-2026-111943; Red Hat Security Bulletin RHSB-2026-012

AFFECTED INTERMEDIATE CERTIFICATE AUTHORITIES

Certificate Name	Purpose	Status
EM DV TLS CA - G3B	Domain-validated TLS	Compromised
EM DV TLS CA - G3C	Domain-validated TLS	Compromised
EM OV TLS CA - G3B	Organization-validated TLS	Compromised
EM OV TLS CA - G3C	Organization-validated TLS	Compromised
EM EV TLS CA - G3B	Extended-validation TLS	Compromised
EM EV TLS CA - G3C	Extended-validation TLS	Compromised
EM OV CS CA - G3B	Code signing	Compromised
EM OV CS CA - G3C	Code signing	Compromised

INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should actively monitor for:

1. Clients or servers trusting emSign ECC Root CA - G3, emSign Root TLS CA - G3, or AAA Certificate Services without the intermediate-specific blocks applied.
2. Applications maintaining independent certificate stores (Java keystores, Python certifi bundles, Node.js deployments, containers).
3. Statically compiled Go binaries built with vulnerable toolchains and not yet rebuilt.
4. SSL inspection proxies, VPN products, security appliances, IoT devices, and legacy applications with outdated trust stores.
5. Production TLS services chaining through emSign ECC Root CA - G3.
6. Certificates chaining to any of the eight compromised intermediates, including Sectigo cross-signed paths.
7. Unexpected TLS issuers, unusual certificate chains, or certificate warnings.
8. Suspicious network redirection or connections using the affected intermediates.
9. Clients that neither enforce Certificate Transparency nor reliably reject revoked certificates.
10. CA bundle or runtime package versions older than the fixed releases listed in this advisory.
11. Presence of the 8 compromised intermediate CA certificates or their Subject Public Key Info (SPKI) SHA-256 fingerprints in custom application keystores, local stores, or active TLS handshakes.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



PKCERT

National Cyber Emergency Response Team

Government of Pakistan



REMEDIATION ACTIONS

1. Priority Response Controls (MANDATORY)

Action Category	Specific Actions
Update Software and Trust Stores	Apply available security releases to operating systems, browsers, servers, developer runtimes, CA bundles, containers, and applications; prioritize internet-facing services, government systems, financial applications, and CII
Distrust Compromised Intermediates	Use vendor-supported intermediate certificate or SPKI blocking; ensure both original and cross-signed certificates are rejected; where intermediate-specific blocking is unavailable, assess root removal per platform guidance
Identify Independent Certificate Stores	Review Java keystores, Python certifi bundles, Go executables, Node.js deployments, containers, SSL inspection proxies, VPN products, security appliances, IoT, and legacy applications
Replace Legitimate Certificates	Identify production TLS services chaining through emSign ECC Root CA - G3 and coordinate reissuance under an unaffected trusted hierarchy before 27 October 2026
Monitor for MITM Activity	Investigate unusual TLS chains, unexpected issuers, certificate warnings, and suspicious redirection; review historical logs where available
Validate and Document	Test representative clients against known revoked chains, verify package and trust-store versions, and document affected assets, compensating controls, exceptions, and remaining risks
Network Appliance CA Updates	update trust stores on Next-Generation Firewalls (NGFWs), Web Application Firewalls (WAFs), Proxy Servers, and Outbound SSL Decryption engines. Manually block the 8 compromised eMudhra intermediates (including Sectigo cross-signed certificates) across all perimeter devices.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



2. Vendor Patch Availability and Remediation Status

Versions and protective actions identified in disclosures available on 21 October 2026. Deployment status must be checked for each product and device.

Platform / Product	Patched Version or Action	Status
Google Chrome	CRLSet SPKI block delivered 17 October; root removal planned 27 October	Initial protection deployed
Mozilla Firefox	158.0.1 (Desktop/Android)	Released
Firefox ESR	115.43.1 / 153.5.1	Released
Mozilla NSS	3.131.1	Released
Apple platforms	Affected intermediates blocked 19 October	Protection reported
Microsoft platforms	Affected intermediates blocked 20 October	Protection reported
Android	Google Play Services security update	Distributed
Go	1.27.3 / 1.26.10	Released
Node.js	22.23.4 / 24.22.1 / 26.12.1	Listed as fixed
Python certifi	2026.10.19	Released
Alpine ca-certificates	20261020-r0	Released
Arch Linux ca-certificates-mozilla	3.131.1-1	Released
curl CA bundle	2026-10-20	Released
Rust rustls-webpki	0.103.16	Released
Rust webpki-roots	1.0.10	Released
Cloudflare	Emergency service-level protections	Deployed

Note: Mozilla and Google provide direct confirmation of their protections. The developer-platform and package versions above are listed by a community-maintained remediation tracker; verify the corresponding upstream release and distribution-specific package before deploying.

Important Operational Note: Updating a browser does not automatically secure Java applications, Python virtual environments, statically compiled Go binaries, Linux containers, embedded systems, or other applications maintaining their own certificate stores. Go applications compiled with vulnerable toolchains must be rebuilt and redeployed with a fixed Go release.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

3. Certificate Trust Paths Requiring Review

Mozilla identified the following relevant trust anchors. The hashes below are SPKI SHA-256 identifiers of roots, not of the eight affected intermediates.

Root / Trust Anchor	SPKI SHA-256
emSign ECC Root CA - G3	8d417db2dd8bf5e3084d1e3f196d583849d81bdd4c00c70b9d39369e96b8c782
emSign Root TLS CA - G3	c619e4780ed8e0abeda24ad732567de4383a7ea941338f6d1a7d1b49ac792fe9
AAA Certificate Services	bd153ed7b0434f6886b17bce8bbe84ed340c7132d702a8f4fa318f756ecbd6f3

Caution: Do not indiscriminately remove these roots across all systems without evaluating certificate dependencies; root removal can invalidate other legitimate certificates unrelated to the weak intermediate keys. A targeted SPKI block of the compromised intermediates is preferable when supported.

4. Technical Verification

Security teams may use the researcher's published test endpoints to determine whether a curl-based client still accepts an affected certificate chain:

Test	Command	Interpretation
Affected DV G3B chain	<code>curl -v https://dv-g3b-emudhra.we-have-a-problem.com/</code>	Validation error = chain rejected
Affected DV G3B chain via AAA root	<code>curl -v https://dv-g3b-aaa-emudhra.we-have-a-problem.com/</code>	Normal successful TLS = client may be vulnerable
Verify Disallowed / Untrusted Certificates Store (Windows)	<code>Get-ChildItem Cert:\LocalMachine\Disallowed</code>	Windows PowerShell

Verification Guidance:

1. Do not use the -k or --insecure option for this validation.
2. These checks are not comprehensive; other applications may use different certificate stores and verification mechanisms.
3. The researcher's technical tracker page includes certificate chains and an affected-intermediate JSON list for comprehensive defensive testing.
4. Retain package and trust-store versions, test results, and exceptions for audit purposes.
5. Windows / Enterprise PKI Verification: Windows administrators can verify that the untrusted/disallowed certificate store has been updated via PowerShell by running: `Get-ChildItem Cert:\LocalMachine\Disallowed`



National Cyber Emergency Response Team

Government of Pakistan



5. Reference Sources and Verification Status

Source	Information Provided	Status
Google	Chrome CRLSet block of the six TLS keys; planned removal of emSign ECC Root CA - G3 (expected 27 October 2026); Android protections; no CT-logged TLS certificates found for the six TLS intermediates	Direct confirmation
Mozilla	OneCRL protections; Firefox and NSS releases; independent recovery of the private keys	Direct confirmation
eMudhra	Revocation of affected intermediates; no legitimate end-entity certificates issued; key-generation flaw statement (investigation ongoing)	Vendor statement
Sectigo	Revocation of affected cross-signed certificates (19 October)	Reported
Red Hat	Advisory RHSB-2026-012 (CVE-2026-111943)	Published 21 October
Community remediation tracker	Developer-platform and package fix versions	Verify upstream

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps
Trust-Store Updates	Update OS, browser, runtime, CA bundle, container, and application trust stores
Intermediate Distrust	Block all eight intermediates, including Sectigo cross-signed paths, via SPKI/intermediate blocking
Independent Store Discovery	Locate applications and devices with their own certificate stores and update them
Certificate Migration	Reissue certificates chaining to emSign ECC Root CA - G3 before 27 October 2026
MITM Monitoring	Investigate abnormal TLS chains, issuers, and redirection
Validation	Test clients against revoked chains and document remaining risk

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

MONITORING & DETECTION REQUIREMENTS

#	Monitoring Activity
1	Monitor TLS connections for certificate chains using any of the eight affected intermediates
2	Detect unexpected certificate issuers and unusual certificate chains
3	Track certificate validation warnings and failures across clients
4	Detect suspicious network redirection or interception of TLS traffic
5	Monitor internal services chaining through emSign ECC Root CA - G3
6	Track patch and trust-store versions across endpoints, servers, containers, and devices
7	Monitor vendor and upstream announcements for updated guidance and the final root-cause findings
8	Retain relevant historical logs to support retrospective investigation

DISASTER RECOVERY & INCIDENT RESPONSE REQUIREMENTS

Phase	Requirement Area	Actions / Controls
1	Incident Identification	Identify unexpected certificate chains or issuers, or clients accepting revoked chains; confirm via TLS logs and validation tests
2	Immediate Containment	Apply SPKI/intermediate blocks; update trust stores on affected clients; isolate affected systems where needed
3	Evidence Preservation	Preserve TLS, proxy, and network logs, certificate chains, and client trust-store versions
4	System Recovery	Patch or rebuild affected software; reissue certificates under an unaffected hierarchy; rotate credentials exposed over potentially intercepted sessions
5	Post-Incident Actions	Report to National CERT Pakistan; review CA trust and certificate-lifecycle management practices

STRATEGIC PROTECTIVE MEASURES (CII & HIGH-VALUE TARGETS)

1. Maintain an inventory of trust stores and certificate-validating applications, including those independent of the operating system.
2. Prefer targeted SPKI blocking of compromised intermediates over wholesale root removal wherever supported.



National Cyber Emergency Response Team

Government of Pakistan



3. Enforce Certificate Transparency checking and reliable revocation checking in clients where feasible.
4. Rebuild and redeploy statically compiled applications (such as Go binaries) with fixed toolchains.
5. Reduce dependence on any single certificate authority by maintaining the ability to reissue certificates under an alternative trusted hierarchy.

INCIDENT REPORTING

All incidents related to suspected forged certificates, interception of TLS traffic, or exploitation of the compromised eMudhra intermediates must be reported to National CERT Pakistan:

- **Incident Reporting Portal:** <https://pkcert.gov.pk/report-incident/>
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Update browsers, operating systems, runtimes, CA bundles, and containers with the available fixes immediately
2	Block all eight compromised intermediates, including cross-signed paths
3	Identify and update applications and devices with independent certificate stores
4	Reissue certificates chaining to emSign ECC Root CA - G3 before 27 October 2026
5	Validate remediation and report incidents to National CERT Pakistan

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk