Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

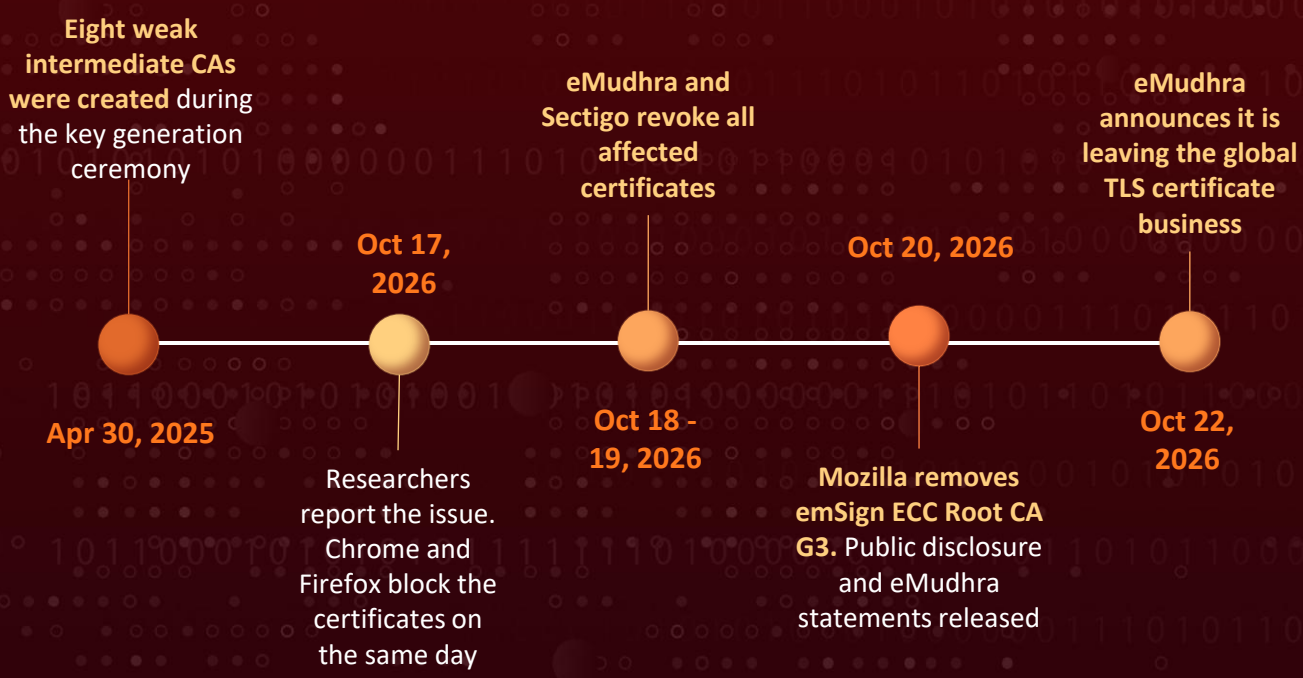
Number Four Holds the Keys: eMudhra Intermediate CA Compromise

Date of Publication	Admiralty Code	TA Number
October 23, 2026	A1	TA2026315

Summary

First Seen: April 30, 2025
Targeted Platforms: Windows, macOS, Linux, Android, Apple platforms, FreeBSD, NetBSD, OpenBSD
Targeted Products: eMudhra emSign intermediate CAs (EM DV TLS CA - G3B, EM DV TLS CA - G3C, EM OV TLS CA - G3B, EM OV TLS CA - G3C, EM EV TLS CA - G3B, EM EV TLS CA - G3C, EM OV CS CA - G3B, EM OV CS CA - G3C) and their Sectigo AAA Certificate Services cross-signs, emSign ECC Root CA - G3, and relying software including Google Chrome, Mozilla Firefox, NSS, Go, Node.js, Python certifi, pip, uv, curl, Rust rustls-webpki and webpki-roots, Electron, Bun, Deno, Docker Desktop, and Linux ca-certificates packages
Attack: Eight eMudhra intermediate CA certificates (six TLS, two code signing) were issued in April 2025 with P-384 private keys whose values were integers below 256, one of them simply the number 4. Anyone holding the public certificates could recover every private key in under a second and forge publicly trusted HTTPS certificates for any domain or sign malicious software. Major browsers blocked the intermediates within hours of the October 17, 2026 report, but non-browser clients that skip revocation checks or ignore Certificate Transparency remain exposed until their trust stores and runtimes are updated. No in-the-wild abuse has been reported so far.

Timeline



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-111943	Go crypto/x509 Trust of Compromised eMudhra Intermediate CA	Go crypto/x509	✗	✗	✓
CVE-2026-113470	Mozilla Firefox Compromised eMudhra Intermediate CA Blocklist Gap	Mozilla Firefox	✗	✗	✓

Attack Details

#1

This was not a breach but a key generation failure. During an April 30, 2025 key ceremony for 24 intermediates, a flawed script created a second, weak set of P-384 keys alongside the strong ones. Because the key labels looked alike, the weak keys were used for eight intermediates, which Sectigo also cross-signed, giving 16 affected certificates. The private keys are the numbers 4, 56, 66, 115, 155, 156, 230, and 237, so anyone can find one by trying at most 256 values.

#2

The flaw went unnoticed for about 17 months and through two audit cycles, even after invalid CRLs for six of the same intermediates in 2025 were re-signed with the weak keys. A researcher reported it on October 17, 2026. Chrome and Firefox blocked the intermediates that day; eMudhra revoked them on October 18, Sectigo revoked the cross-signs, and Apple and Microsoft followed on October 22.

#3

With a TLS key, an attacker can forge a certificate for any website and intercept or alter traffic while the victim sees a valid padlock. With the two code-signing keys, malware could appear to come from a trusted publisher on Windows systems that skip revocation checks. Browsers are protected, and Google found no rogue certificates in Certificate Transparency logs. The risk lies with non-browser clients that use outdated trust stores and skip revocation, such as older Go builds, Python certifi, Node.js, macOS's built-in curl, containers, VPN clients, proxies, and IoT devices.

#4

Intercepted sessions could expose SSO, VPN, and API credentials, or let attackers impersonate package registries to push tampered software into build pipelines. No abuse has been reported as of October 21, 2026, and eMudhra says none of the eight intermediates issued customer certificates. Still, the keys are now public, and past misuse against clients that do not check Certificate Transparency cannot be ruled out.

#5

About 30,800 legitimate certificates chain to the emSign ECC Root CA - G3, which Mozilla has removed and Chrome will remove around October 27, 2026, so they must be replaced. Fixes are tracked as CVE-2026-111943 (Go) and CVE-2026-113470 (Firefox). On October 22, 2026, eMudhra announced it will exit the global SSL/TLS business; its Indian DSC and eSign services were not affected.

Recommendations

Update Language Runtimes and CA Bundles: Move to Go 1.27.3 or 1.26.10, Node.js 22.23.4, 24.22.1 or 26.12.1, Python certifi 2026.10.19, pip 26.2.2, uv 0.13.4, webpki-roots 1.0.10, rustls-webpki 0.103.16, NSS 3.131.1, Electron 44.9.1, 43.8.1 or 42.11.16, Deno 2.9.8, Bun 1.4.4 and Docker Desktop 4.96.2 or later. Go 1.25 and older will not receive a fix.

Rebuild Go Binaries and Container Images: Existing Go binaries keep the old trust behavior, so recompile them with a patched toolchain. Rebuild container images from patched base images and restart services so the new trust material is actually loaded.

Patch Operating System Trust Stores: Apply the ca-certificates updates for Debian, Ubuntu (USN-8944-1, USN-8944-2), Alpine, Fedora, Arch, Gentoo, FreeBSD, OpenBSD and Homebrew. On RHEL 7 and later, apply the RHSB-2026-012 workaround until packages ship, and treat RHEL/UBI-based containers, RHEL CoreOS, OpenShift and OpenStack Platform as potentially affected.

Update Firefox Where Remote Settings Is Disabled: Firefox installations that cannot receive OneCRL updates by policy or network restriction must move to Firefox 158.0.1, ESR 153.5.1 or ESR 115.43.1. Firefox for Android needs 158.0.2 or later, and Snap-packaged browsers on Ubuntu update their root store separately.

Distrust the Compromised Intermediates on Unpatched Systems: On Windows hosts that miss automatic CTL updates, place all 16 intermediate and cross-signed certificates in the LocalMachine\Disallowed store so both Schannel TLS and Authenticode reject them. On Linux and BSD systems that cannot be patched promptly, distrust emSign ECC Root CA - G3 through the distribution's blocklist mechanism, and test before removing AAA Certificate Services because that root still anchors legitimate connections.

Fix macOS Built-in curl Trust: Apple's /usr/bin/curl reads /etc/ssl/cert.pem and does not check revocation. Remove the affected roots from that bundle on managed macOS hosts, point pip3 to the updated bundle with PIP_CERT, and keep certifi upgraded for Python environments.

Replace Certificates Chaining to emSign ECC Root CA - G3:
Site owners whose chain ends at emSign ECC Root CA - G3 (SHA256 86A1ECBA089C4A8D3BBE2734C612BA341D813E043CF9E8A862CD5C57A36BBE6B) must obtain a replacement from another hierarchy trusted by the Chrome Root Store before October 27, 2026. Renew manually, since standard ACME clients will not replace certificates outside their renewal window unless they support ARI, and confirm client configuration when switching from ECC to RSA. Weigh the fact that eMudhra's remaining RSA root is under Chrome review before migrating to it.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.004: Digital Certificates
		T1588.003: Code Signing Certificates
	T1587: Develop Capabilities	T1587.003: Digital Certificates
Credential Access	T1557: Adversary-in-the-Middle	
	T1649: Steal or Forge Authentication Certificates	
Defense Impairment	T1553: Subvert Trust Controls	T1553.002: Code Signing
Impact	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	42C4ACCD12C4F59597925E1A08A7A90102608543809308D50EC427E118BA1493, 45A883F349AEDFD5F3A649B5498FFB121712BA8B448F3F2A91DBC5A766FCDDBE, 0164D7CEAE5BB909C272AF151FF44B1177AE9B47D9424B94F1D9558C30934D19, 62B7F9868263F72F6911FC78CEAF72C1979158B7368BF648683BB2AA39B02E72, E7568FE6E12331F4FD7DE61DA4C7559D0F8EB192A218D4741A3BA75184333838, 579480AEA166290BD3C643589E795FC0D0E54E86505D180F1DFF99EFD3199512, 432EC25F0D28DE9006D97BF752F17BBB2CD41F669933FCB072D9A1148D0261F3, FD9D5C2DBBD4995AB69B8D50C439D9527B00529199C2FD01B2174EB58F07021F, 98B896625C0C230ADEEC3EB2CF6AAD5001ECF9156A68644E82374CE5833BC25B, 5F1DED4DD590AF74631290CF073B122A2AAC6A1FA479778A0BD43579BD832699, CB6E15165AC802E9B3F993F16C25D41F4E81C21EBDE71AE1B012AC00BF9C7C3F, 7485B51C0ED192878FA1D2F948FB529AE1842CC5086C4B67F7BE5B2039DE9489, 9E39DE2881273ACC225A149C72BA3E0F51424963669AB633EE1DC7DF5DB067B4, A496E23AC0CAB8155FC9B117B97EAE368EFCBB9041AEC8804D5A308D2D01C2D8, 4B2460A466F95FD40113BCDCCA2CEB29B3B093921DE45474DA7DF48874C630B1, 84112972B8E59D14560AE7E7119654474AAD119990CF3722BFC1E3B91615E1FD
SPKI SHA256	EBED6475C2C2D80FCB199F3FE8DD6E6B3CE60B77EB15D4E42C3DEC0C6F5B5105, 49DD353DC2B919A3770645117D0E60C16115E7D1BC259EEFE734B00EA434FE5F, E0254C7FCDC265E2F0F8A428DABB75AB4AE039B4872D62F5EE57F0877D5A8A41, 5C0660A2B164910D8FF589C18E14552E9E0EC237DCEFE2CB736D41A4811F81A0, 43BFFA19D6EF651451F6841E019931E96F6F2EAEFF28AB4B6F1CE4576DE2717B,

TYPE	VALUE
SPKI SHA256	63ECEFEE431D49523BC1136C4E72D0206A477086CAF606CD5CF025686C109CF8, EC4FFA1AD0AC88081314B7AAFFEF6A91F97CD57291BB5BA686C5415F5EB4F6B6, 92C063D67E8F14DB71D288E11266FFDAF69CBF115F7BAB14F3BC2F68D25E0E30
Certificate Serial	c7c41efe92d825f05eae841a4a82c1, 6cada367fb1c100088120ea202d568, a4aee678f23362b4c0e460b772f214, 8009928a64107601af05fa2f19f109, 296926c227a3a1526392b19482a504, 588b2e3c2bb8cda13e1a1209254321, 7818933f8f85b4619a2b35fba83d0a, 544b7f922c31ae220a4a922916f6e6, d8f8685e4f2bd9d82402a85a1c1eb731, e94223bde92f914e5ab9acabfdac3710, a024fdf4ba665c785ce4a020483858b7, 05f078752dece7a1bb8595d303167171, 8d5a4811939ef447d77111cdd9849ae9, 91f347f1a5b7d39962b95e0ee4e299d1, 41e32b73ac185d6ce0d7480bacf84e69, d6a5ef613b390f32ef9cdf349f772841

Patch Details

CVE-2026-113470:
https://www.mozilla.org/en-GB/security/advisories/mfsa2026-111/#CVE-2026-113470

CVE-2026-111943:
https://go-review.googlesource.com/c/go/+/851047

https://github.com/golang/go/issues/82345

References

https://emudhra.we-have-a-problem.com/

https://bugzilla.mozilla.org/show_bug.cgi?id=2083449

https://www.bseindia.com/xml-data/corpfiling/AttachLive/6be0c423-b335-494b-86f3-54c561c3a5f9.pdf

https://blog.google/security/protecting-chrome-and-android-users-from-compromised-emudhra-intermediate-ca-certificates/

https://blog.talosintelligence.com/compromised-intermediate-certificates/

https://unit42.paloaltonetworks.com/emudhra-certificate-compromise/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

October 23, 2026 • 02:00 PM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com