

eMudhra revokes eight weak-key CA certificates; browsers and OS vendors block them



eMudhra revoked eight intermediate CA certificates whose private keys were trivially recoverable. Browsers have blocked them, but software with its own trust stores may still accept them until updated.

- Eight intermediate certificates used P-384 keys generated in April 2025 with values below 256, so they could be recovered by testing 256 numbers.
- eMudhra attributed the flaw to a script error; weaker keys were mistakenly chosen for signing. It reports no evidence of issuance to end users.
- Mozilla and Chrome blocked the certificates on October 17, Apple on October 19; Firefox 158.0.1 followed on October 20.
- Software using its own certificate stores or skipping revocation checks may still trust them; Go

fixed this in CVE-2026-111943.

- macOS's built-in `/usr/bin/curl` may keep trusting the certificates.

What happened

Certificate authority eMudhra revoked eight intermediate certificates after a researcher found, on October 17, that their private keys were extremely weak. According to Mozilla's incident report, the P-384 keys were generated in April 2025 with values below 256, so anyone could recover them by testing 256 possibilities. A published example showed a key value of just 4. BleepingComputer verified that the published key matches one of the revoked certificates.

eMudhra attributed the problem to an error in its generation script, which produced a second set of weaker keys that were mistakenly picked for signing because their labels resembled the correct ones. Some certificates were also submitted to Sectigo for cross-signing. The company says most of the intermediates were never used in production and it found no evidence of certificates issued to end users. Abuse since April 2025 was possible, though there is no evidence it occurred.

Vendor response

Mozilla blocked the certificates via OneCRL on October 17 without needing a browser update. Chrome blocked the six intermediates authorized for TLS that day, and Apple added protections on October 19. Mozilla released Firefox 158.0.1 and ESR updates on October 20 for configurations that could not receive the earlier revocation.

The remaining exposure lies in software with its own certificate stores or no revocation checking. Go released versions 1.27.3 and 1.26.10 for CVE-2026-111943. A tracking site by Mozilla engineer Dennis Jackson lists affected software and fixes, and warns that macOS's built-in `/usr/bin/curl` may still trust the certificates.

Why it matters

Forged certificates could let an attacker impersonate legitimate sites and intercept encrypted traffic. Browsers are largely covered; applications, servers and containers are where gaps are likely.

What to do now

1. Inventory applications, servers, containers and build images that bundle their own CA stores or skip revocation checks.
2. Apply the CA bundle and runtime updates listed on the incident tracking site, including Go 1.27.3 or 1.26.10 where relevant.
3. Update Firefox to 158.0.1 or the current ESR release, and confirm Chrome and Apple devices are current.
4. Use the advisory's test endpoints to confirm which systems still trust the revoked intermediates.

5. Do not rely on macOS's built-in `/usr/bin/curl` for trust-sensitive tasks until it is addressed.
6. Record the exercise in your certificate and vulnerability management records.