ELO TOUCH SOLUTIONS

Product Security Advisory

Compromise of eMudhra Intermediate Certificate Authorities

Advisory ID	ELO-SA-2026-eMudhra-ICA
Publication Date	October 2026
Last Updated	October 29, 2026
Severity	Informational — Monitoring
Status	Mitigated via vendor OS updates
Issuer	Elo Touch Solutions — Product Security Response Team (PSRT)

Executive Summary

Elo Touch Solutions is actively monitoring and addressing an industry-wide cryptographic vulnerability involving eMudhra Technologies Limited, a commercial Certificate Authority (CA).

On October 17, 2026, security researchers disclosed that private keys associated with eight intermediate CA certificates operated by eMudhra were generated with critical cryptographic defects (extremely weak entropy of only 3 to 8 bits), allowing third parties to immediately deduce the private signing keys. The potential impact to Elo customers is isolated to Elo enterprise Android and Windows product lines.

The scope of automatic protection is important to understand:

- **Android 14 devices with Google Mobile Services (GMS) and active Google Play Services:** Automatically protected through the emergency Google Play Services component update released on October 19, 2026. No customer action is required.
- **All other Android OS versions (Android 13 and below), AOSP-only builds, and non-GMS devices:** Google will provide the fix for these platforms as a patch update rather than through the Play Services component channel. Elo will incorporate that patch update into an OS firmware update, qualify it, and publish it for the affected Elo device models. These devices are NOT automatically protected until the Elo OS firmware update is released and installed. Until that firmware update is available, administrators must apply the manual mitigation plan described later in this advisory.
- **Windows devices:** Automatically protected through the Microsoft Windows Disallowed Certificate Trust List update of October 20, 2026 and an automatic CRLSet update for Microsoft Edge and WebView2. No customer action is required.

No other Elo products are affected. Elo's corporate infrastructure, cloud services (EloView, Elo Radar, and Elo Remote), and internal systems are not compromised. At the time of this advisory, there have been no reports of active exploitation against Elo customers.

Summary at a Glance

- **Issue:** A critical cryptographic flaw was disclosed involving eight eMudhra intermediate Certificate Authorities, potentially allowing attackers to spoof secure websites or forge trusted signatures.
- **Impact:** Impact is limited to Elo enterprise Android and Windows devices; all other Elo products and solutions are unaffected. This vulnerability originated strictly within eMudhra's external key generation process. Elo infrastructure, cloud platforms, and internal systems are completely secure and uncompromised.
- **Resolution for Android - Android 14 GMS devices:** For Elo Android 14 devices running Google Mobile Services with active Google Play Services, protection has already been delivered silently and automatically via the emergency Google Play Services component update of October 19, 2026 and background browser revocation updates. No customer action, firmware flashing, or OS update is required.
- **Resolution for Android - Other Android OS Versions:** For all other Android OS versions (Android 13 and below), AOSP-only builds, and non-GMS devices, Google will provide the fix as a patch update rather than through the Play Services component channel. Elo will qualify that patch update and publish a corresponding OS firmware update for the affected Elo device models. These devices are NOT automatically protected until the Elo OS firmware update is released and installed. Until then, administrators must apply the manual mitigation plan described in this advisory.
- **Resolution for Windows:** No customer action is required. On October 20, 2026, Microsoft published an update to the Windows Disallowed Certificate Trust List to block the affected intermediate certificate authorities. Microsoft also deployed a separate CRLSet update for Microsoft Edge and WebView2 to block the affected TLS certificates. The Edge and WebView2 update is delivered automatically through the component update mechanism and does not require customers to install a new browser version.
- For detailed information on Windows products, refer to the Microsoft Response to Compromised eMudhra Certificate Authority Keys Blog.

Additional Details: Android Remediation

For Elo enterprise Android devices, remediation depends on the Android OS version, the presence of Google Mobile Services (GMS), and the software application stack in use:

- **Browsers (Google Chrome):** Automatically protected on all supported Android versions via background browser revocation list updates (CRLSets/OneCRL) and strict Certificate Transparency

(CT) enforcement. Google Chrome has revoked trust for the affected public key hashes via out-of-band updates.

- **Native Apps and WebView on Android 14 GMS devices (including Elo's WebView Controller):** Automatically protected via the emergency component update pushed by Google Play Services on October 19, 2026, which added the eMudhra certificates to the Revocation List (blocklist) of Android's system trust store. Google Play Services must be enabled on the device for this update to be delivered.
- **Native Apps and WebView on other Android OS versions, AOSP, and non-GMS devices:** Not covered by the Play Services component update. Google will provide the fix as a patch update for these platforms, which Elo will incorporate into an OS firmware update, qualify, and publish for the affected Elo device models. Until that Elo OS firmware update is released and installed, the manual mitigation plan described below must be applied.

For further technical background, refer to the Google Security Blog: Protecting Chrome and Android Users from Compromised eMudhra Intermediate CA Certificates.

Detailed Impact Analysis by Architecture on Android

1. Android Web Browsers (Google Chrome)

Chrome manages its own independent root store and does not rely on the underlying Android OS trust store. For browser-based applications, the protection is enforced directly within the browser application itself.

Because Chrome manages its own independent trust store, manually removing or disabling the certificates from the Android OS Trust Store will not impact Chrome's behavior. Chrome has pushed updates that block the compromised eMudhra certificates by adding them to its internal revocation list (CRLSet), which applies silently and instantly upon internet connection.

Additionally, Chrome natively enforces Certificate Transparency (CT). Because no legitimate certificates were ever logged for these compromised keys before the revocation, any attempt by an attacker to present a forged certificate will be rejected instantly by Chrome due to the lack of valid Signed Certificate Timestamps (SCTs).

2. Android Native Applications using WebView

An Android system-level update is necessary for applications that access web endpoints directly rather than via a standalone browser. The most common implementation is through the WebView control API, which is utilized by Elo WebView Controller.

For Android 14 devices with Google Mobile Services (GMS) and active Google Play Services, Google has delivered an automatic component update that appends the eight compromised eMudhra intermediate public key hashes to Android's secure blocklist. This update requires no administrative intervention and no OS-level firmware update. During technical validation on Elo Android 14 GMS devices, the secure

blocklist entries arrived in just over one second after a factory-reset device was connected to the internet.

For all other Android OS versions (Android 13 and below), AOSP-only builds, and non-GMS devices, this Play Services component update is not available. Google will provide the equivalent protection as a patch update for these platforms. Elo will qualify that patch update and publish a corresponding OS firmware update for the affected device models. Until the Elo OS firmware update is released and installed, administrators must apply the manual mitigation plan described in the next section.

Manual Mitigation Plan (Required Until OS Firmware Update is Available)

The following manual mitigation plan applies to any Elo Android device that is not an Android 14 GMS device with active Google Play Services. This includes Android 13 and below, AOSP-only builds, non-GMS devices, and devices operating in restricted networks where the Play Services component update cannot be delivered. These devices will receive the full fix only when Google releases the corresponding patch update and Elo publishes an OS firmware update incorporating that patch for the affected device models, and that firmware update is installed on the device; until that happens, administrators must apply the steps below.

Elo is actively tracking Google's patch update availability for each affected Android OS version and will qualify and publish the corresponding firmware for Elo device models as soon as it is received. In the interim, administrators should apply the network- and application-level controls below.

Network-Level Compensating Control

For enterprises managing large fleets where manual configuration is not immediately practical, it is highly recommended to implement an inspection rule on local corporate firewalls or secure web gateways (such as Zscaler, Palo Alto Networks, Fortinet, etc.). The rule should block any inbound or outbound connections presenting certificates signed by the compromised eMudhra intermediate keys, serving as an immediate network barrier while local device configurations are updated.

Manual Certificate Disabling Procedure

1. Navigate to **Settings > Security** (or **Security Privacy > More Security Settings**).
2. Select **Encryption credentials** > **Trusted credentials**.
3. Under the **System** tab, locate and toggle Disable on the following two root certificates (disabling these covers both the direct chains and the Sectigo cross-signed variants):
    - **emSign ECC Root CA - G3** (Listed under **eMudhra Technologies Limited**)
    - **AAA Certificate Services** (Listed under **Comodo CA Limited**)

> **Note:** Disabling these roots secures Android system TLS and WebView applications, but standalone browsers like Chrome will continue to rely on their own automatic internal updates.

Verification and Testing Endpoints

Security administrators can validate local device and network-level security behaviors by navigating to the independent test endpoints established for this incident:

- **Primary Compromised Intermediate Test:** https://dv-g3b-emudhra.we-have-a-problem.com/
- **General Incident Reference and Test Suite:** https://emudhra.we-have-a-problem.com/

Other Elo Products and Services

Elo interactive touchscreen displays, signage, point-of-sale systems, peripherals, and backend management tooling do not utilize or trust the affected eMudhra certificate chains and are completely unaffected by this incident.

Elo cloud services (including EloView, Elo Radar, and Elo Remote) do not use eMudhra-issued certificates. As a precaution, Elo is proactively updating its server-side trust stores to distrust the affected root certificates. Elo Android and Windows hardware products are fully aligned with the operating system and browser guidance detailed above.

References

- Microsoft Response to Compromised eMudhra Certificate Authority Keys
- Google Security Blog: Protecting Chrome and Android Users from Compromised eMudhra Intermediate CA Certificates

Contact Information

Elo Website: https://www.elotouch.com

Elo Customer Support: https://www.elotouch.com/support

Disclaimer

Update delivery times vary by region, device model, and third-party supplier. Some updates may require the operating system to be running the latest maintenance release before the fix is applied. This advisory is provided on an "as-is" basis for informational purposes only; Elo Touch Solutions disclaims all warranties, either express or implied, including implied warranties of merchantability and fitness for a particular purpose. Elo reserves the right to update this advisory as additional information becomes available.

© 2026 Elo Touch Solutions, Inc. All rights reserved.
Elo Touch Solutions and the Elo logo are trademarks of Elo Touch Solutions, Inc.