Three country-code registries hijacked to obtain HTTPS certificates for Google domains



Google said attackers compromised the .gh, .sl and .as registries and obtained unauthorized HTTPS certificates for several Google domains. Google's own systems were not breached, but domains under those three endings were put at risk.

- Google said on October 6 that attackers compromised three country-code top-level domains: .gh (Ghana), .sl (Sierra Leone) and .as (American Samoa).
- The attackers obtained unauthorized HTTPS certificates for several Google domains.
- Google's own systems were not breached.
- Any domain ending in .gh, .sl or .as was put at risk.
- A fraudulent certificate could let an attacker pose as the genuine site over an encrypted connection.

What happened

Google said on October 6 that attackers compromised three country-code top-level domains (ccTLDs): .gh for Ghana, .sl for Sierra Leone and .as for American Samoa. Using that access, they obtained unauthorized HTTPS certificates for several Google domains.

Google stated that its own systems were not breached. The weakness lay at the registry level, which put any domain ending in .gh, .sl or .as at risk.

Why it matters

A valid certificate for a domain lets whoever holds it pose as the real site over an encrypted connection. Users would see no obvious warning, because the certificate would appear legitimate. The incident shows that trust in HTTPS depends partly on the security of registries and the processes that validate domain control, which sit outside an organization's own perimeter.

The source does not describe how the registries were compromised, how many certificates were issued, or whether other organizations were affected. Readers should treat the details as limited until further information is published.

What to consider

Institutions in the Kingdom are unlikely to be directly exposed unless they own or depend on domains under these three endings. Even so, the case is a useful prompt to review domain inventories, certificate monitoring and third-party dependencies, and to confirm that the team knows how to respond if a fraudulent certificate is found for one of its own domains.

What to do now

1. Check whether your organization or key suppliers own or depend on domains ending in .gh, .sl or .as.
2. Review Certificate Transparency logs for your domains and confirm that unexpected certificate issuance triggers an alert.
3. Maintain a complete inventory of domains, registrars and registry accounts, with multi-factor authentication on registrar access.
4. Consider CAA records to restrict which certificate authorities may issue certificates for your domains.
5. Include fraudulent-certificate discovery in your incident response playbook, covering revocation and notification steps.