
Official Statement Regarding the Reported .sl Registry Security Incident

12 October 2026

CoCCA (CoCCA Registry Services (NZ Limited) acknowledges the press release issued by Sierra Leone's Ministry of Communication, Technology & Innovation on 9 October 2026 concerning a security breach affecting the country's .sl country-code top-level domain (ccTLD) registry.

According to the Ministry's press release, the incident occurred on 25 September 2026 and involved unauthorized access to a domain registry they described as the CoCCA domain management system.

Given the reference to CoCCA in the Ministry's statement, we consider it is important to clarify, that while the .sl ccTLD may be operating a locally modified variant of the free software that CoCCA last made available in May 2015, more than 11 years ago, any version of CoCCA software currently operated by the .sl registry is outdated, unsupported, and not maintained by CoCCA.

CoCCA has never had , and does not currently have any agreement with the .sl registry for technical support, software patches, security updates, and operational assistance. CoCCA has no visibility into which version of the software currently deployed by the .sl registry, how it has been configured and maintained, or whether any updates or modifications have been made over the years.

Important Clarification Regarding CoCCA's Current Platform

The reported incident should not be presented as evidence of a compromise of CoCCA's current supported platform or infrastructure. The incident concerns a registry operating outside CoCCA's contractual support arrangements, potentially using outdated software in a configuration and hosting environment over which CoCCA has no visibility, control, or responsibility.

It is essential to distinguish between the legacy versions of CoCCA software made freely available for ccTLD administrator more than 11 years ago, and CoCCA's current, actively maintained and supported registry management solutions.

References to the "CoCCA domain management system" without making this distinction may create a misleading impression that CoCCA's current software, infrastructure or other supported services were involved in the reported incident.

Security and Operational Considerations

Dated, unsupported versions of CoCCA software should be considered insecure and should not be relied upon for the operation of critical registry infrastructure without appropriate security assessment, end user modification, maintenance and support. Using software that has not received ongoing maintenance patches and security updates may expose registry operators to vulnerabilities and operational risks.

Incident Investigation

CoCCA has not participated in the investigation of the reported incident and has not received any technical information to establish its cause. Accordingly, CoCCA cannot confirm whether the incident resulted from a software vulnerability, system configuration, operational practices, infrastructure breach or other factors.

Recommendation to ccTLD Operators

CoCCA strongly advises any ccTLD operator still running the last freely available version of CoCCA software, released in May 2015, or any other outdated and unsupported version, to conduct an immediate review of its software, infrastructure, security configurations and operational practices.

Outdated and unsupported registry management software should be considered a significant security risk, particularly where critical infrastructure is operated without ongoing maintenance, regular security assessments or access to timely security patches.

CoCCA urges all ccTLD operators using legacy software to take proactive steps to assess and mitigate potential vulnerabilities and ensure their registry systems are appropriately maintained, secured and protected against evolving cybersecurity threats. CoCCA remains committed to the security, reliability and continued development of its registry management solutions and to supporting the operators that rely on its services.

We believe accurate and responsible communication regarding cybersecurity incidents is essential. In particular, a clear distinction must be maintained between historical software releases, independently operated and modified deployments, local hosting environments and CoCCA's current supported platform and infrastructure.

For further information or clarification: info@coccaregistry.org.