مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in AWS-LC Cryptographic Library

Tracking #:432318526

Date:06-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in AWS-LC, an open-source cryptographic library used by various AWS services and applications, which may impact cryptographic validation and encryption processes.

TECHNICAL DETAILS:

Amazon Web Services has disclosed multiple vulnerabilities in **AWS-LC**, an open-source cryptographic library used by AWS services and applications. Successful exploitation may allow attackers to bypass certificate or signature validation mechanisms or perform timing side-channel analysis.

Vulnerabilities Details

High Severity

- **PKCS7_verify Certificate Chain Validation Bypass – CVE-2026-3336**
  Improper certificate validation may allow attackers to bypass certificate chain verification when processing PKCS7 objects with multiple signers.
- **Timing Side-Channel in AES-CCM Tag Verification – CVE-2026-3337**
  Timing discrepancies during AES-CCM decryption may allow attackers to infer authentication tag validity through timing analysis.
- **PKCS7_verify Signature Validation Bypass – CVE-2026-3338**
  Improper signature validation may allow attackers to bypass signature verification when processing PKCS7 objects with authenticated attributes.

Affected Versions

- PKCS7_verify Certificate Chain Validation Bypass in AWS-LC >= v1.41.0, < v1.69.0
- PKCS7_verify Certificate Chain Validation Bypass in aws-lc-sys >= v0.24.0, < v0.38.0
- Timing Side-Channel in AES-CCM Tag Verification in AWS-LC >= v1.21.0, < v1.69.0
- Timing Side-Channel in AES-CCM Tag Verification in AWS-LC >= AWS-LC-FIPS-3.0.0, < AWS-LC-FIPS-3.2.0
- Timing Side-Channel in AES-CCM Tag Verification in aws-lc-sys >= v0.14.0, < v0.38.0
- Timing Side-Channel in AES-CCM Tag Verification in aws-lc-sys-fips >= v0.13.0, < v0.13.12
- PKCS7_verify Signature Validation bypass in AWS-LC >= v1.41.0, < v1.69.0
- PKCS7_verify Signature Validation bypass in aws-lc-sys >= v0.24.0, < v0.38.0

Fixed Versions

- **AWS-LC:** v1.69.0 or later
- **AWS-LC-FIPS:** v3.2.0 or later
- **aws-lc-sys:** v0.38.0 or later
- **aws-lc-sys-fips:** v0.13.12 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by AWS.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://aws.amazon.com/security/security-bulletins/rss/2026-005-aws/