مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Memory Disclosure Vulnerability in OpenSSL

Tracking #:432318751

Date:08-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a vulnerability identified as CVE-2026-31790 affects multiple versions of OpenSSL's 3.x branch, specifically within the RSA Key Encapsulation Mechanism (KEM) using RSASVE.

TECHNICAL DETAILS:

A vulnerability identified as CVE-2026-31790 affects multiple versions of OpenSSL's 3.x branch, specifically within the RSA Key Encapsulation Mechanism (KEM) using RSASVE. The flaw arises from improper validation of encryption return values, allowing failed operations to be interpreted as successful.

Vulnerability Details:

- CVE ID: CVE-2026-31790
- Severity: Moderate
- Affected Component: RSA KEM (RSASVE) implementation
- Affected Function: RSA_public_encrypt()
- Attack Vector: Remote (via crafted public keys)
- Impact: Sensitive data exposure (memory disclosure)

Affected Products:

- OpenSSL 3.0.x
- OpenSSL 3.3.x
- OpenSSL 3.4.x
- OpenSSL 3.5.x
- OpenSSL 3.6.x
- Associated FIPS modules

Unaffected Versions:

- OpenSSL 1.0.2
- OpenSSL 1.1.1

Fixed Version:

- OpenSSL 3.0.20
- OpenSSL 3.3.7
- OpenSSL 3.4.5
- OpenSSL 3.5.6
- OpenSSL 3.6.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to fixed version.

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://openssl-library.org/news/secadv/20260407.txt