مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

OpenSSL Security Updates – January 2026

Tracking #:432318323

Date:29-01-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The OpenSSL Project has released security update addressing multiple vulnerabilities across supported OpenSSL versions.

TECHNICAL DETAILS:

The OpenSSL Project has released a security update addressing multiple vulnerabilities across supported OpenSSL versions. The most severe issue, CVE-2025-15467, is a high-severity, pre-authentication stack buffer overflow that may allow remote code execution (RCE) or denial of service (DoS).
The vulnerability is particularly dangerous because it can be triggered without valid credentials or cryptographic keys, making internet-facing systems and services especially at risk. Additional vulnerabilities include flaws in PKCS#12 file handling, TLS 1.3 memory management, CMS parsing, and QUIC cipher handling.
Organizations using OpenSSL for TLS, certificate handling, CMS processing, or cryptographic services are strongly advised to upgrade immediately.

Vulnerability Details:

1. CVE-2025-15467 – Stack Buffer Overflow in CMS AuthEnvelopedData
    - Severity: High
2. CVE-2025-11187 – PKCS#12 MAC Verification Flaw
    - Severity: Moderate

3. Additional Low-Severity Vulnerabilities
    - CVE-2025-15469 – Data Truncation in openssl dgst
    - CVE-2025-66199 – TLS 1.3 Memory Exhaustion
    - CVE-2025-15468 – NULL Pointer Dereference (QUIC)

Affected Versions

The following OpenSSL branches are impacted:

- OpenSSL 3.6.x
- OpenSSL 3.5.x
- OpenSSL 3.4.x
- OpenSSL 3.3.x
- OpenSSL 3.0.x
- Legacy versions 1.1.1 and 1.0.2 (premium support only)

Remediation & Fixed Versions

Organizations should upgrade immediately to the following patched releases:

- OpenSSL 3.6 → 3.6.1
- OpenSSL 3.5 → 3.5.5
- OpenSSL 3.4 → 3.4.4
- OpenSSL 3.3 → 3.3.6
- OpenSSL 3.0 → 3.0.19
- OpenSSL 1.1.1 / 1.0.2 → Vendor-provided patched builds

RECOMMENDATIONS:

- Upgrade OpenSSL immediately on all affected systems.

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/20260127.txt