مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in OpenSSL

Tracking #:432317767

Date:01-10-2025

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 OpenSSL has released security updates addressing multiple vulnerabilities affecting multiple OpenSSL versions.

TECHNICAL DETAILS:

OpenSSL has released security updates addressing multiple vulnerabilities affecting multiple OpenSSL versions. While each vulnerability has different exploitation scenarios, they pose risks ranging from Denial of Service (DoS) to remote code execution and potential private key exposure. Organizations running affected OpenSSL versions are strongly advised to apply vendor-provided patches immediately.

Vulnerability Details

1. **CVE-2025-9230** – Out-of-bounds Read/Write in RFC 3211 KEK Unwrap
    - Severity: Moderate
    - Affected Versions: OpenSSL 3.5, 3.4, 3.3, 3.2, 3.0, 1.1.1, 1.0.2
    - Impact:
        - Crash → Denial of Service (DoS)
        - Memory corruption → Possible remote code execution
    - Exploitation Likelihood: Low (since password-based CMS encryption is rarely used)
    - Patched Versions:
        - 3.5.4, 3.4.3, 3.3.5, 3.2.6, 3.0.18
        - 1.1.1zd & 1.0.2zm (Premium support only)

2. **CVE-2025-9231** – Timing Side-Channel in SM2 (64-bit ARM)
    - Severity: Moderate
    - Affected Versions: OpenSSL 3.5, 3.4, 3.3, 3.2
    - Impact:
        - Potential private key recovery through timing analysis of SM2 signature computations
        - May be exploitable remotely in certain custom provider contexts
    - Exploitation Likelihood: Medium (context-dependent, requires timing access)
    - Patched Versions:
        - 3.5.4, 3.4.3, 3.3.5, 3.2.6

3. **CVE-2025-9232** – Out-of-bounds Read in HTTP client no_proxy Handling
    - Severity: Low
    - Affected Versions: OpenSSL 3.5.0+, 3.4.0+, 3.3.3+, 3.2.4+, 3.1.8+, 3.0.16+
    - Impact:
        - Crash → Denial of Service (DoS)
        - Requires attacker-controlled URL *and* specific no_proxy configuration
    - Exploitation Likelihood: Very low (complex conditions required)
    - Patched Versions:
        - 3.5.4, 3.4.3, 3.3.5, 3.2.6, 3.0.18

RECOMMENDATIONS:

- Apply Security Updates Immediately- Upgrade OpenSSL to the latest patched versions.

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.

REFERNCES:

- https://openssl-library.org/news/secadv/20250930.txt