EnCyb

Severity: High

Advisory Type: Security

Multiple Security Vulnerabilities in OpenSSL

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

OpenSSL has released security updates addressing multiple vulnerabilities affecting OpenSSL 3.x releases, including issues in cryptographic message parsing that could be exploited via crafted CMS, PKCS#7, or PKCS#12 inputs. Organizations using OpenSSL to process untrusted cryptographic data are strongly advised to upgrade to the latest patched versions to mitigate the risk of denial-of-service, memory corruption, or potential code execution.

- Total CVE: 12
- Active Region: Global
- Affected Sector: IT, Cloud Services, Web Hosting, Enterprise Applications, Email & PKI Services
- Affected Product: OpenSSL (versions 3.0–3.6; some CVEs also affect 1.1.1 and 1.0.2 premium releases)
- Severity: High (1), Moderate (1), Low (10)
- Published Date: January 28, 2026

CVE LIST

SL.NO	CVE-ID	Description	Severity
1	CVE-2025-15467	Stack buffer overflow in CMS AuthEnvelopedData parsing (AEAD / AES-GCM)	High
2	CVE-2025-11187	Stack buffer overflow due to improper PBMAC1 validation in PKCS#12	Moderate
3	CVE-2025-15468	Null pointer dereference in QUIC cipher suite lookup	Low
4	CVE-2025-15469	Data truncation in openssl dgst when processing inputs larger than 16MB	Low
5	CVE-2025-66199	Excessive memory allocation via TLS 1.3 certificate compression	Low
6	CVE-2025-68160	Heap out-of-bounds write in BIO linebuffer handling	Low
7	CVE-2025-69418	OCB mode may leave trailing bytes unencrypted under specific conditions	Low
8	CVE-2025-69419	Out-of-bounds write in PKCS#12 friendlyName parsing	Low

9	CVE-2025-69420	Null pointer dereference in timestamp verification	Low
10	CVE-2025-69421	Null pointer dereference in PKCS#12 decryption	Low
11	CVE-2026-22795	Type confusion vulnerability in PKCS#12 processing	Low
12	CVE-2026-22796	Type confusion vulnerability in PKCS#7 digest handling	Low

AFFECTED AND FIXED VERSION(S)

SL.NO	CVE-ID	Affected Versions	Fixed Version(s)
1	CVE-2025-15467	3.0, 3.3, 3.4, 3.5, 3.6	3.0.19, 3.3.6, 3.4.4, 3.5.5, 3.6.1
2	CVE-2025-11187	3.4, 3.5, 3.6	3.4.4, 3.5.5, 3.6.1
3	CVE-2025-15468	3.5, 3.6	3.5.5, 3.6.1
4	CVE-2025-15469		
5	CVE-2025-66199	3.3, 3.4, 3.5, 3.6	3.3.6, 3.4.4, 3.5.5, 3.6.1
6	CVE-2025-68160	1.0.2 – 3.6	Latest supported release (>= 3.0.19 / 3.6.1)
7	CVE-2025-69418	3.5, 3.6	3.5.5, 3.6.1
8	CVE-2025-69419		
9	CVE-2025-69420		
10	CVE-2025-69421		
11	CVE-2026-22795		
12	CVE-2026-22796		

TECHNICAL DETAILS - HIGH & MODERATE VULNERABILITIES

CVE-2025-15467 - Stack buffer overflow in CMS AuthEnvelopedData parsing (AEAD / AES-GCM)

- Attack Vector: Remote, unauthenticated attacker sends a crafted CMS/PKCS#7 message containing an oversized Initialization Vector (IV).
- Cause: Improper bounds checking of AEAD (e.g., AES-GCM) IV length during CMS AuthEnvelopedData parsing, leading to a stack buffer overflow.
- Prerequisite: Target application must parse untrusted CMS/PKCS#7 or S/MIME content using vulnerable OpenSSL versions

CVE-2025-11187 - Stack buffer overflow due to improper PBMAC1 validation in PKCS#12

- Attack Vector: Local or remote attack via a maliciously crafted PKCS#12 (.p12/.pfx) file processed by the target application.
- Cause: Improper validation of PBMAC1 parameters during PKCS#12 verification, allowing an excessive key length to overflow a fixed-size stack buffer.

- Prerequisite: User or service must import, open, or verify an untrusted PKCS#12 file using vulnerable OpenSSL versions (3.4–3.6).
- Risk: Application crash (denial of service) or potential code execution when handling malicious PKCS#12 files.

IMPACT

- Possible remote code execution
- Application crashes leading to DoS
- Memory corruption (stack/heap overflows)
- Excessive memory usage and resource exhaustion
- Data integrity loss due to truncation
- Weakened encryption guarantees
- Risk when handling untrusted cryptographic inputs

RECOMMENDATIONS

- Apply Upgrade OpenSSL immediately to the latest patched versions (3.6.1, 3.5.5, 3.4.4, 3.3.6, 3.0.19)
- Prioritize patching systems that process untrusted CMS, PKCS#7, PKCS#12, or S/MIME data
- Avoid importing untrusted PKCS#12 files until systems are fully patched
- Disable TLS 1.3 certificate compression where not required to reduce DoS risk
- Audit application dependencies to identify bundled or statically linked OpenSSL versions

REFERENCE

- https://cyberpress.org/openssl-vulnerabilities-remote-execute-malicious-code/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com