An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611200235

NCSC Advisory

Critical Vulnerability in OpenSSL

CVE-2026-121481

20th, November 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-121481

Published: 2026-11-18

Vendor: OpenSSL

Product: OpenSSL

CVSS Score[1]: 9.8

Products Affected

Product	Version
OpenSSL	4.1.0 < 4.1.1
OpenSSL	4.0.0 < 4.0.4

Impact

Calling EVP_EncodeBlock() with an input length close to INT_MAX may overflow the calculation of the encoded output size and write past the end of the caller-supplied output buffer. No path by which an attacker can trigger this has been identified. An application that passes an input length near INT_MAX to EVP_EncodeBlock() could suffer a heap buffer overflow, crashing or corrupting its own memory, but it must itself supply such a length.

Description: EVP_EncodeBlock() base64-encodes a buffer of a caller-supplied length into an output buffer that the caller allocates. The caller is expected to reserve 4*((len+2)/3)+1 bytes. For input lengths close to INT_MAX, the arithmetic that computes the encoded length overflows a signed integer, so the function writes more data than the documented output size. The result is a heap buffer overflow in the calling process. Reaching this requires an application to pass an input length near INT_MAX to EVP_EncodeBlock(). OpenSSL's TLS, QUIC and CMS implementations never encode buffers of that size, and the command line tools cannot practically be made to do so: the limits on reading a proxy password from a file and on bignum sizes prevent it. An application that accepts an attacker-controlled length and forwards it to EVP_EncodeBlock() without its own bound check is exposed.

[1] https://www.first.org/cvss/

Common Weakness Enumeration (CWE)[2]: CWE-190: CWE-190 Integer Overflow or Wraparound, CWE-122: CWE-122 Heap-based Buffer Overflow

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from OpenSSL.

- https://nvd.nist.gov/vuln/detail/CVE-2026-121481
- https://www.cve.org/CVERecord?id=CVE-2026-121481
- https://github.com/openssl/openssl/pull/33652

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog