OpenSSL out-of-bounds write via integer overflow in EVP_EncodeBlock

CVSS: 9.8 Critical CISA-ADP

Share

Affects OpenSSL 4.0.0 before 4.0.4 and 4.1.0 before 4.1.1, only when an application calls EVP_EncodeBlock() with a length whose encoded size overflows an int. Fixed in 4.0.4 and 4.1.1.

CVE-2026-121481 · EUVD-2026-12682 · GHSA-83XJ-7XH4-4P7X

Published November 18, 2026, updated Nov 20, 2026

Exploited	Fix	Who is exposed
No known exploitation	Fixed in 4.1.1, 4.0.4	Not reported

Summary

Calling EVP_EncodeBlock() in OpenSSL with an input length close to INT_MAX can overflow the calculation of the encoded output size. This causes writes past the end of the caller-supplied output buffer.

Written by a model

Original description

Issue summary: 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.

Impact summary: 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.

CWE: CWE-190: Integer Overflow or Wraparound

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.

The severity is Low because no attacker-controlled path to the overflow is known. The caller must already hold a buffer of about two gigabytes before the defect can be reached.

FIPS impact: no The affected code is outside the FIPS module boundary.

Who should check

Teams whose own code calls OpenSSL EVP_EncodeBlock() with input lengths near INT_MAX (about 2 GB), without a length bound check.

"lengths for which the encoded size does not fit in an int"

github.com

Details

Last checked	Nov 20, 2026
EPSS score	0.31% · 24th percentile
Attack conditions	Unclear
Vendor severity	Low (openssl)
Public exploit	1 proof of concept on GitHub
CISA SSVC	Automatable: yes (Attackers can reliably automate reconnaissance, weaponization, delivery and exploitation.) · Technical impact: total (An attacker gains total control over the software or total disclosure of its information.).
CVSS vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H openssl rates this low ·
On X	View the cve.now post

What to do

Upgrade to a fixed version: 4.1.1, 4.0.4.

Check your systems with an agent

Paste this into a coding or ops agent. It checks your systems read-only and reports a table per asset.

```
Check whether my systems are affected by CVE-2026-121481 (Integer Overflow in EVP_En

Rules: work read-only. Do not run exploit code, proof-of-concept scripts or scanners

What cve.now has for CVE-2026-121481 (entry last updated 2026-11-20):
Affected:
- OpenSSL OpenSSL: from 4.1.0, fixed in 4.1.1; from 4.0.0, fixed in 4.0.4
Fixed versions: 4.1.1, 4.0.4.
Conditions (all must be true for the bug to be hit):
- The application calls EVP_EncodeBlock() with a length whose encoded size does not
Setup: unknown whether the bug needs a non-default feature or setting. Check the adv
Attacker needs: network access, no login, no user action.
CISA KEV: CVE-2026-121481 is not listed as of cve.now's last read.
This KEV status is for CVE-2026-121481 only. If you also check another CVE, look up

How to check:
- Installed software: check what is actually running, not what a repo declares. Read

Verify against the linked advisories before concluding, and cite the date you read e
- https://github.com/openssl/openssl/pull/33652
- https://news.ycombinator.com/item?id=58569226
Do not conclude an asset is unaffected unless you checked it and the evidence covers

Report a table with one row per asset and these columns: Asset | Version or build | T

Entry: https://cve.now/CVE-2026-121481
For follow-up questions, use the cve.now MCP server at https://mcp.cve.now/mcp (no a
```

Affected versions

OpenSSL OpenSSL
From 4.1.0 · fixed in 4.1.1; From 4.0.0 · fixed in 4.0.4

cve.now Index

50 /100 · provisional · methodology v3

Exploitation	0/40	No signal
Exposure	20/25	No login or user action needed, CISA rates it automatable · *Unknown: Advisories don't say whether default setups are affected.*
Reach	20/20	Affects OpenSSL (software on nearly every server, desktop or phone)
Severity	10/10	CVSS 9.8, total technical impact per CISA
No patch	0/5	No signal

What would change the score

- Would score about 95 if added to CISA KEV
- Would score about 90 if CISA's SSVC rates exploitation active
- Would score about 55 if advisories confirm default setups are exposed

How the score works · Rankings

Timeline

Nov 18, 2026, 12:43 PM GMT+1
CVE published

Nov 18, 2026, 1:18 PM GMT+1
First seen by cve.now

1 day

Nov 19, 2026, 10:20 PM GMT+1
CISA SSVC assessment
Exploitation: none · Automatable: yes · Technical impact: total

Nov 19, 2026, 10:42 PM GMT+1
Posted on X by cve.now

1 day

Nov 20, 2026, 11:13 AM GMT+1
Record last updated

Evidence 5

CVE record 2
Establishes: The identifier and description.

Record	CVE List · CVE-2026-121481 ↗
	NVD · CVE-2026-121481 ↗

Public exploit code 1
Establishes: Public exploit code exists (Exploit-DB, Metasploit, Nuclei and GitHub).

Exploit	GitHub · Quarendir/openssl-cve-2026-121481-audit · Repository ↗

Other links 2

Patch	GitHub · openssl/openssl · Pull request #33652 ↗
Link	news.ycombinator.com · item?id=50569226 ↗

Questions about CVE-2026-121481

Is CVE-2026-121481 being exploited?

What does this mean?

Which versions are affected by CVE-2026-121481?

Am I affected, and how do I check?

How do I fix CVE-2026-121481?

Why is it rated 9.8 Critical?

Sources

CVE List ↗
CVE Terms of Use

National Vulnerability Database ↗
NVD terms of use

ENISA European Vulnerability Database ↗
ENISA terms of use

PoC-in-GitHub ↗
CC0-1.0

Related

CVE-2026-107494
Unbounded QUIC RETIRE_CONNECTION_ID Frame Sending Queue

CVE-2026-84782
DTLS Retransmits Handshake Messages From a Stale Buffer Offset

CVE-2026-95691
Retransmitted QUIC CRYPTO Frames Can Cause DoS or One-byte Disclosure

CVE-2026-107493
Use-After-Free in PEM_X509_INFO_read_bio_ex() when appending to a caller-supplied stack fails

CVE-2026-84786
Possible NULL Dereference in Non-SMTP DANE Clients

CVE-2026-121482
Verifying a maliciously crafted CMS or PKCS#7 SignedData message with CRL checking enabled...

OpenSSL vulnerabilities

OpenSSL CVEs

CVEs published in November 2026

CVEs published in 2026

CISA KEV catalog

Highest EPSS scores today

No corrections so far. Something wrong on this page? Report an error

Want to know which of these affect your systems? Sazabi can tell you.

cve.now

CVEs
Advisories
Early warnings
Breaches
Vendors
Packages
Tech
Latest
Rankings
Daily
Live
PR check

Vendors

Linux
Microsoft
Oracle
Google
IBM
Adobe
Apple
Cisco
All vendors

Ecosystems

npm
PyPI
Go
Maven
crates.io
Packagist
RubyGems
Hex
NuGet

For agents

Agents
RSS
llms.txt
Status

Labs

Sazabi
down.guide

About

About
X
GitHub

Data: CVE List, GitHub Advisory Database, OSV, NVD, ENISA EUVD, CISA KEV, FIRST EPSS, Exploit-DB. Summaries CC-BY 4.0. Uses NVD data; not endorsed by NVD. Critical · CISA KEV catalog · EPSS scores