# Stack buffer overflow in CMS (Auth)EnvelopedData parsing

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2025-15467 |
| **State** | PUBLISHED |
| **Assigner** | openssl |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-01-27 16:16:14 UTC |
| **Updated** | 2026-05-07 18:12:43 UTC |
| **Description** | Issue summary: Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters |

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**Problem Types:** CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | ADP | DECLARED | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |

### CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Openssl | Openssl | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | OpenSSL | OpenSSL | affected 3.6.0 3.6.1 semver | Not specified |
| CNA | OpenSSL | OpenSSL | affected 3.5.0 3.5.5 semver | Not specified |
| CNA | OpenSSL | OpenSSL | affected 3.4.0 3.4.4 semver | Not specified |
| CNA | OpenSSL | OpenSSL | affected 3.3.0 3.3.6 semver | Not specified |
| CNA | OpenSSL | OpenSSL | affected 3.0.0 3.0.19 semver | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| github.com/guiimoraes/CVE-2025-15467 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | github.c |
| github.com/openssl/openssl/commit/6ced0fe6b10faa560e410e3ee8d6c82f06c65ea3 | openssl-security@openssl.org | github.c |
| github.com/openssl/openssl/commit/ce39170276daec87f55c39dad1f629b56344429e | openssl-security@openssl.org | github.c |
| github.com/openssl/openssl/commit/5f26d4202f5b89664c5c3f3c62086276026ba9a9 | openssl-security@openssl.org | github.c |
| openssl-library.org/news/secadv/20260127.txt | openssl-security@openssl.org | openssl- |
| github.com/openssl/openssl/commit/d0071a0799f20cc8101730145349ed4487c268dc | openssl-security@openssl.org | github.c |
| www.openwall.com/lists/oss-security/2026/01/27/10 | af854a3a-2127-422b-91ae-364da2661108 | www.op |
| www.openwall.com/lists/oss-security/2026/02/25/6 | af854a3a-2127-422b-91ae-364da2661108 | www.op |
| github.com/openssl/openssl/commit/2c8f0e5fa9b6ee5508a0349e4572ddb74db5a703 | openssl-security@openssl.org | github.c |
| CVE Program record | CVE.ORG | www.cv |
| NVD vulnerability detail | NVD | nvd.nist. |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Stanislav Fort (Aisle Research) (en)

**CNA:** Igor Ustinov (en)

There are currently no legacy QID mappings associated with this CVE.



**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**