



# Possible NULL Dereference When Processing CMS KeyAgreeRecipientInfo

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-28389
<b>State</b>	PUBLISHED
<b>Assigner</b>	openssl
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-07 22:16:21 UTC
<b>Updated</b>	2026-04-08 21:27:00 UTC
<b>Description</b>	Issue summary: During processing of a crafted CMS EnvelopedData message with KeyAgreeRecipientInfo a NULL pointer

## Risk And Classification

**EPSS:** 0.000290000 probability, percentile 0.084220000 (date 2026-04-09)

**Problem Types:** CWE-476 | CWE-476 CWE-476 NULL Pointer Dereference

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.6.0 3.6.2 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.5.0 3.5.6 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.4.0 3.4.5 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.3.0 3.3.7 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.0.0 3.0.20 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 1.1.1 1.1.1zg custom	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 1.0.2 1.0.2zp custom	Not specified

## References

Reference	Source	Link
<a href="https://openssl-library.org/news/secadv/20260407.txt">openssl-library.org/news/secadv/20260407.txt</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="https://openssl-library.org">openssl-library.org</a>
<a href="https://github.com/openssl/openssl/commit/16cea4188e0ea567deb4f93f85902247e67384f5">github.com/openssl/openssl/commit/16cea4188e0ea567deb4f93f85902247e67384f5</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/openssl/openssl/commit/785cbf7ea3b5a6f5adf0c1ccb92b79d89c35c616">github.com/openssl/openssl/commit/785cbf7ea3b5a6f5adf0c1ccb92b79d89c35c616</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/openssl/openssl/commit/f80f83bc5fd036bc47d773e8b15a001e2b4ce686">github.com/openssl/openssl/commit/f80f83bc5fd036bc47d773e8b15a001e2b4ce686</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/openssl/openssl/commit/7b5274e812400cacb6f3be4c2df5340923fa807f">github.com/openssl/openssl/commit/7b5274e812400cacb6f3be4c2df5340923fa807f</a>	<a href="mailto:openssl-security@openssl.org">openssl-security@openssl.org</a>	<a href="https://github.com">github.com</a>

github.com/openssl/openssl/commit/c6725634e089eb2b634b10ede33944be7248172a	openssl-security@openssl.org	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

- Discovery Credit
- CNA:** Nathan Sportsman (Praetorian) (en)
  - CNA:** Daniel Rhea (en)
  - CNA:** Jaeho Nam (Seoul National University) (en)
  - CNA:** Muhammad Daffa (en)
  - CNA:** Zhanpeng Liu (Tencent Xuanwu Lab) (en)
  - CNA:** Guannan Wang (Tencent Xuanwu Lab) (en)
  - CNA:** Guancheng Li (Tencent Xuanwu Lab) (en)
  - CNA:** Joshua Rogers (en)
  - CNA:** Neil Horman (en)

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

© [CVE.report](https://cve.report) 2026 |  
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.  
CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).  
**Free CVE JSON API** [cve.report/api](https://cve.report/api)  
**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)