Possible NULL Dereference When Processing CMS KeyAgreeRecipientInfo

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

Summary

CVE	CVE-2026-28389
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 22:16:21 UTC
Updated	2026-04-08 21:27:00 UTC
Description	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	OpenSSL	OpenSSL	affected 3.6.0 3.6.2 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.5.0 3.5.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.4.0 3.4.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.3.0 3.3.7 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.20 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1zg custom	Not specified
CNA	OpenSSL	OpenSSL	affected 1.0.2 1.0.2zp custom	Not specified

References

Reference	Source	Link
openssl-library.org/news/secadv/20260407.txt	openssl-security@openssl.org	openssl-library.org
github.com/openssl/openssl/commit/16cea4188e0ea567deb4f93f85902247e67384f5	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/785cbf7ea3b5a6f5adf0c1ccb92b79d89c35c616	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/f80f83bc5fd036bc47d773e8b15a001e2b4ce686	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/7b5274e812400cacb6f3be4c2df5340923fa807f	openssl-security@openssl.org	github.com

github.com/openssl/openssl/commit/c6725634e089eb2b634b10ede33944be7248172a	openssl-security@openssl.org	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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.