Possible NULL Dereference When Processing CMS KeyTransportRecipientInfo

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

Summary

CVE	CVE-2026-28390
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 KeyTransportRecipientInfo a NULL poir

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/01194a8f1941115cd0383bfa91c736dd3993c8bc	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/fd2f1a6cf53b9ceeca723a001aa4b825d7c7ee75	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/2e39b7a6993be445fddb9fbce316fa756e0397b6	openssl-security@openssl.org	github.com
github.com/openssl/openssl/commit/af2a5fecd3e71a29e7568f9c1453dec5cebbaff4	openssl-security@openssl.org	github.com

github.com/openssl/openssl/commit/ea7b4ea4f9f853521ba34830cbcadc970d2e0788	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: 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: Chanho Kim (en)

CNA: Neil Horman (en)

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