Out-of-bounds Read in AES-CFB-128 on X86-64 with AVX-512 Support

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

Summary

CVE	CVE-2026-28386
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 22:16:20 UTC
Updated	2026-04-08 21:27:00 UTC
Description	Issue summary: Applications using AES-CFB128 encryption or decryption on systems with AVX-512 and VAES support car

Risk And Classification

EPSS: 0.000190000 probability, percentile 0.050600000 (date 2026-04-09)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSSL	OpenSSL	affected 3.6.0 3.6.2 semver	Not specified

References

Reference	Source	Link	T
openssl-library.org/news/secadv/20260407.txt	openssl-security@openssl.org	openssl-library.org	
github.com/openssl/openssl/commit/61f428a2fc6671ede184a19f71e6e495f0689621	openssl-security@openssl.org	github.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

Vendor Comments And Credit

Discovery Credit

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Pavel Kohout (Aisle Research) (en)

CNA: Alex Gaynor (Anthropic) (en)

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Pavel Kohout (Aisle Research) (en)

CNA: Alex Gaynor (Anthropic) (en)

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