ALVD-2026-366

ID alternative: CVE-2026-45447

8.8 || I LARTË

PËRSHKRIM

Cenueshmëri e tipit Use-After-Free në funksionin PKCS7_verify() të OpenSSL. Kur përpunohet një mesazh i firmosur PKCS#7 ose S/MIME në të cilin fusha digestAlgorithms është e pranishme si një ASN.1 SET bosh, OpenSSL mund të lirojë gabimisht një objekt BIO në pronësi të aplikacionit thirrës. Përdorimi i mëpasshëm i këtij BIO-je (zakonisht gjatë thirrjes BIO_free()) shkakton një gjendje use-after-free, e cila mund të çojë në rrëzim të procesit, dëmtim të heap-it ose potencialisht ekzekutim kodi në distancë. Aplikacionet që përdorin API-të CMS për këtë përpunim nuk preken.

KRITIKALITETI

CVSS Base Score: 8.8 (I lartë)
Versioni CVSS: 3.1

PUBLISHED

09.06.2026

VENDOR

OpenSSL

PRODUCT

OpenSSL

VERSION

OpenSSL 1.0.2 - 4.0.0

MASAT E REKOMANDUARA

Përditësimi i menjëhershëm i OpenSSL në një nga versionet e rregulluara ose më të reja: 3.0.21, 3.4.6, 3.5.7, 3.6.3, 4.0.1, sipas degës që përdoret, i cili e adreson plotësisht vulnerabilitetin.

PRODUKTI I PREKUR

PRODHUESI	PRODUKTI	VERSIONI	ZGJIDHUR	PUBLIKUAR
OpenSSL	OpenSSL	OpenSSL 1.0.2 - 4.0.0	3.0.21 3.4.6 3.5.7 3.6.3 4.0.1	09.06.2026

REFERENCA

- https://euvd.enisa.europa.eu/vulnerability/CVE-2026-45447
- https://www.cve.org/CVERecord?id=CVE-2026-45447