ALVD-2026-361

ID alternative: CVE-2026-34182

9.1 || KRITIK

PËRSHKRIM

Cenueshmëri në përpunimin e mesazheve CMS (Cryptographic Message Syntax) të OpenSSL, e cila dështon të kryejë validim të mjaftueshëm të fushave të shifrës dhe të gjatësisë së tag-ut në kontejnerët AuthEnvelopedData. Një sulmues mund të specifikojë një shifër jo-AEAD (p.sh. AES-256-OFB) ose të reduktojë gjatësinë e tag-ut në një bajt të vetëm, duke anashkaluar kontrollet e integritetit. Kjo i mundëson sulmuesit të falsifikojë përmbajtje të besuar ose, nëpërmjet një orakulli sukses/dështim, të arrijë funksionalitet ekuivalent me çelësin për marrësin e zgjedhur të mesazhit.

KRITIKALITETI

CVSS Base Score: 9.1 (Kritik)
Versioni CVSS: 3.1

PUBLISHED

09.06.2026

VENDOR

OpenSSL

PRODUCT

OpenSSL

VERSION

OpenSSL 3.0 - 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 3.0 - 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-2026-34182
- https://www.cve.org/CVERecord?id=CVE-2026-34182