AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësia e Zbulimit të Memories në OpenSSL

Data: 09/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Një dobësi e identifikuar si CVE-2026-31790 prek versione të shumta të 3.x të OpenSSL, konkretisht brenda Mekanizmit të Enkapsulimit të Çelësave RSA (KEM) duke përdorur RSASVE.

Informacione Teknike

Një dobësi e identifikuar si CVE-2026-31790 ndikon në versione të shumta të degës 3.x të OpenSSL, konkretisht brenda Mekanizmit të Enkapsulimit të Çelësave RSA (KEM) duke përdorur RSASVE. Dobesia rrjedh nga validimi i gabuar i vlerave të kthimit të enkriptimit, duke lejuar që operacionet e dështuara të interpretohen si të suksesshme.

Detajet e dobësisë:
• ID e CVE: CVE-2026-31790
• Ashpërsia: Moderate
• Komponenti i prekur: Implementimi i RSA KEM (RSASVE)
• Funksioni i prekur: RSA_public_encrypt()
• Vektori i sulmit: Në distancë (nëpërmjet çelësave publikë të krijuar)
• Ndikimi: Ekspozimi ndaj të dhënave sensitive (zbulimi i memories)
Produktet e prekura:
• OpenSSL 3.0.x
• OpenSSL 3.3.x
• OpenSSL 3.4.x
• OpenSSL 3.5.x
• OpenSSL 3.6.x
• Modulet FIPS të lidhura

Versionet e paprekura:
• OpenSSL 1.0.2
• OpenSSL 1.1.1

Versioni i përditësuar :
• OpenSSL 3.0.20
• OpenSSL 3.3.7
• OpenSSL 3.4.5
• OpenSSL 3.5.6
• OpenSSL 3.6.2

Rekomandime

AKSK rekomandon përditësimin e versioneve te afektuara menjëherë