AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi të Shumta në Apache Tomcat

Data: 14/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Janë identifikuar disa dobësi në Apache Tomcat që mund të rrezikojnë sigurinë e të dhënave dhe mekanizmave të autentikimit.

Informacione Teknike

Dobësitë Kryesore

Rrezikshmëri e Lartë

CVE-2026-29146 – Sulm Padding Oracle në EncryptInterceptor

- Komponenti **EncryptInterceptor** është i cenueshëm ndaj një sulmi padding oracle
- Lejon sulmuesit të dekriptojnë të dhëna sensitive pa pasur çelësin e enkriptimit

CVE-2026-34486 – Anashkalim i EncryptInterceptor (gabim në patch)

- Një gabim në korrigjimin e CVE-2026-29146 lejon anashkalimin e EncryptInterceptor
- Rezulton në ekspozim të të dhënave sensitive në formë të paenkriptuar

Rrezikshmëri Mesatare

CVE-2026-34500 – Anashkalim i autentikimit përmes OCSP Soft-Fail

- Autentikimi **CLIENT_CERT** mund të kalojë gabimisht kur ndodhin gabime në validimin OCSP
- Edhe kur sjellja soft-fail është çaktivizuar

Versionet e Korrigjuara

- **Apache Tomcat 11.0.21** ose më i ri
- **Apache Tomcat 10.1.54** ose më i ri
- **Apache Tomcat 9.0.117** ose më i ri

Rekomandime

Rekomandohet aplikimi i masave zbutëse ose zgjidhjeve alternative të ofruara nga Apache Tomcat.

Referenca

https://lists.apache.org/thread/lzt04z2pb3dc5tk85obn80xygw3z1p0w
https://lists.apache.org/thread/9510k5p5zdvt9pkkgtyp85mvwxo2qrly
https://lists.apache.org/thread/7rcl4zdxryc8hy3htyfyxkbqpxjtfdl2