AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi për Anashkalim të Sigurisë dhe Zbulim të Informacionit Sensitiv në Apache ZooKeeper

Data: 09/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 1
Referenca 1

Përmbledhje Ekzekutive

Janë identifikuar disa dobësi në **Apache ZooKeeper**. Këto dobësi (**CVE-2026-24281** dhe **CVE-2026-24308**) mund t'u lejojnë sulmuesve të anashkalojnë mekanizmat e verifikimit të hostname dhe të ekspozojnë sekrete sensitive përmes log-eve të sistemit.

Nëse shfrytëzohen, këto dobësi mund t'u mundësojnë sulmuesve:

- të imitojnë hoste të besuara
- të marrin kredenciale të ruajtura në skedarët e konfigurimit

Informacione Teknike

Detaje të Dobësisë:

1. Authentication / Hostname Verification Bypass

- **CVE ID:** CVE-2026-24281
- **Komponenti:** ZKTrustManager
- **Lloji i dobësisë:** Validim i pasaktë i certifikatës / Authentication Bypass

2. Sensitive Information Disclosure via Logs

- **CVE ID:** CVE-2026-24308
- **Komponenti:** ZKConfig
- **Lloji i dobësisë:** Zbulim informacioni (Information Disclosure)

Versionet e cenueshme	Versioni i rregulluar
3.9.0 – 3.9.4	3.9.5
3.8.0 – 3.8.5	3.8.6

Rekomandime

AKSK rekomandon të përditësoni **ZooKeeper** në versionet e rregulluara.

Referenca

https://nvd.nist.gov/vuln/detail/CVE-2026-24281