



**AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE**

Vulnerabilitet kritik në Everest Forms WordPress Plugin

Data: 14/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive	2
Informacione Teknike	2
Rekomandime	2

Përmbledhje Ekzekutive

Një dobësi kritike (CVE-2026-3296) me një rezultat CVSS prej 9.8 (Kritik) është identifikuar në plugin Everest Forms WordPress, duke prekur mbi 100,000 faqe interneti.

Informacione Teknike

Një dobësi kritike (CVE-2026-3296) me një rezultat CVSS prej 9.8 (Kritik) është identifikuar në plugin Everest Forms WordPress, duke prekur mbi 100,000 faqe interneti. Gabimi u lejon sulmuesve të paautorizuar të kryejnë injeksion të objekteve PHP, duke çuar potencialisht në ekzekutimin e kodit në distancë (RCE), kompromentimin e plotë të faqes dhe instalimin e vazhdueshëm të backdoor

Problemi është i shfrytëzueshëm në mënyrë aktive përmes formularëve publikë, duke mos kërkuar autentifikim, duke e bërë atë shumë të rrezikshëm për mjediset e ekspozuara.

Detajet e dobësisë

- ID e CVE: CVE-2026-3296
- Ashpërsia: Kritike (CVSS 9.8)
- Softuer i prekur: Plugin Everest Forms WordPress ≤ v3.4.3
- Versioni i rregulluar: v3.4.4
- Lloji i dobësisë: Injeksion i objekteve PHP (Deserializim i pasigurt)

Rekomandime

AKSK rekomandon përditësimin e plugin-it Everest Forms WordPress në versionin e përditësuar ose më të ri menjëherë.