AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi Kritike në Nginx UI

Data: 10/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 2
Referenca 2

Përmbledhje Ekzekutive

Së fundi është identifikuar një dobësi kritike në **Nginx UI**, e cila lejon aktorë keqdashës pa autentikim të shkarkojnë dhe deshifrojnë kopje rezervë të plota të sistemit nga serverët e prekur.

Informacione Teknike

Është identifikuar një dobësi kritike në **Nginx UI** që u mundëson aktorëve keqdashës pa autentikim të shkarkojnë dhe deshifrojnë kopje rezervë të plota të sistemit nga serverët e prekur. Dobësia, e gjurmuar si **CVE-2026-27944**, ka marrë një vlerësim **CVSS 9.8 (Kritike)**.

Kjo dobësi u mundëson sulmuesve të marrin të dhëna të ndjeshme, duke përfshirë:

- kredenciale përdoruesish
- skedarë konfigurimi të sistemit
- token-e sesioni
- çelësa privatë SSL/TLS

Kjo mund të çojë potencialisht në **kompromet**im **të plotë të mjedisit të serverit të prekur**.

Detajet e Dobësisë:

Identifikuesi i dobësisë
CVE-2026-27944

Ashpërsia
Kritike (CVSS Score: 9.8)

Produkti i prekur
Nginx UI

Versionet e prekura:
Versionet para **2.3.2**

Versioni i korrigjuar:
Versioni **2.3.3**

Rekomandime

AKSK rekomandon të përditësoni **Nginx UI** në versionin e korrigjuar ose në një version më të ri.

Referenca

https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-g9w5-qffc-6762