



AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Përditësim Sigurie – Dell ThinOS 10

Data: 10/02/2026

Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive	1
Informacione Teknike	1
Rekomandime	1
Referenca	2

Përmbledhje Ekzekutive

Së fundi, Dell ka publikuar përditësime sigurie për ThinOS 10 për të adresuar disa dobësi kritike që prekin komponentë të palëve të treta, përfshirë OpenSSL, Samba, Google Chrome dhe Amazon WorkSpace Client. Këto dobësi mund t'u mundësojnë aktorëve keqdashës të komprometojnë sistemet thin client të prekura, duke çuar potencialisht në **akses të paautorizuar, ekspozim të të dhënave, ndërprerje shërbimi (DoS)** ose **ekzekutim kodi nga distanca (RCE)**.

Informacione Teknike

Komponentë të Palëve të Treta të Prekur

Rrezikshmëria: KRITIKE

1. Dobësi në OpenSSL

- **CVE ID:** CVE-2025-9232, CVE-2025-9231, CVE-2025-9230
- **Komponenti:** Libraria kriptografike OpenSSL

2. Dobësi në Samba

- **CVE ID:** CVE-2025-10230, CVE-2025-9640
- **Komponenti:** Shërbimi i ndarjes së skedarëve Samba

3. Dobësi në Google Chrome

- **CVE ID:** CVE-2025-13223, CVE-2025-13226, CVE-2025-13227, CVE-2025-13228, CVE-2025-13229, CVE-2025-13230, CVE-2025-12036
- **Komponenti:** Shfletuesi web Google Chrome (7 dobësi të veçanta)

4. Dobësi në Amazon WorkSpace Client

- **CVE ID:** CVE-2024-47601, CVE-2024-47602, CVE-2024-47603
- **Komponenti:** Amazon WorkSpace Client

Produktet dhe Versionet e Prekura:

Komponenti	Versionet e Cenueshme	Versioni i Rregulluar
ThinOS 10 Core	Të gjitha versionet < 2511_10.0380	2511_10.0380 ose më i ri

Komponenti	Versionet e Cenueshme	Versioni i Rregulluar
Google Chrome	Versioni 141.0.7390.76.279_T10 dhe më herët	143.0.7499.169.301_T10 ose më i ri
Amazon WorkSpace Client	Versioni 2025.0.4484.220_T10 dhe më herët	2025.1.5526.236_T10 ose më i ri

Rekomandime

AKSK rekomandon të **përditësoni Dell ThinOS 10** në versionin e rregulluar ose më të ri.

Referenca

<https://www.dell.com/support/kbdoc/en-us/000415990/dsa-2026-056>