AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Përditësime Sigurie – Cisco

Data: 05/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Cisco ka publikuar përditësime sigurie që adresojnë dobësi të shumta që prekin **TelePresence dhe RoomOS Software**, **Cisco Meeting Management**, **Cisco Secure Web Appliance**, **Cisco Prime Infrastructure** dhe **Cisco Evolved Programmable Network Manager (EPNM)**.

Këto dobësi variojnë nga **Denial of Service (DoS)** dhe **ngarkim arbitrar skedarësh**, deri te **Cross-Site Scripting (XSS)** dhe **Open Redirect**, duke u mundësuar potencialisht sulmuesve të ndërpresin shërbime, të ngarkojnë skedarë keqdashës ose të kryejnë sulme në anën e klientit.

Informacione Teknike

Detaje të Dobësisë:

1. Cisco TelePresence Collaboration Endpoint Software dhe RoomOS – Denial of Service (DoS)

- **CVE ID:** CVE-2026-20119
- **Rrezikshmëria:** E lartë
- Ekziston një dobësi për shkak të trajtimit të pasaktë të kërkesave të formuara posaçërisht nga rrjeti. Një sulmues i paautentikuar nga distanca mund ta shfrytëzojë këtë dobësi për të shkaktuar një gjendje DoS, duke e bërë pajisjen të papërgjegjshme dhe duke kërkuar rinisje manuale për rikuperim.

2. Cisco Meeting Management – Ngarkim Arbitrar Skedarësh

- **CVE ID:** CVE-2026-20098
- **Rrezikshmëria:** E lartë
- Cisco Meeting Management përmban një dobësi të ngarkimit arbitrar të skedarëve për shkak të validimit të pamjaftueshëm të skedarëve të ngarkuar. Një sulmues i autentikuar mund ta shfrytëzojë këtë dobësi për të ngarkuar skedarë keqdashës, duke çuar potencialisht në ekzekutim kodi nga distanca, kompromet im sistemi ose akses të paautorizuar në të dhëna sensitive.

3. Cisco Secure Web Appliance – Anashkalim i Skanimit në Kohë Reale të Arkivave

- **CVE ID:** CVE-2026-20056
- **Rrezikshmëria:** Mesatare
- Ekziston një dobësi që lejon arkiva të formuara posaçërisht të anashkalojnë skanimin në kohë reale për malware. Një sulmues mund ta shfrytëzojë këtë për të shpërndarë përmbajtje keqdashëse që nuk inspektohet siç duhet.

4. Cisco Prime Infrastructure – Stored Cross-Site Scripting (XSS)

- **CVE ID:** CVE-2026-20111
- **Rrezikshmëria:** Mesatare
- Një dobësi në ndërfaqen web të menaxhimit mund t'i lejojë një sulmuesi të autentikuar të kryejë një sulm stored XSS. Dobësia vjen nga validimi i pamjaftueshëm i input-it, duke i lejuar një përdoruesi me kredenciale administrative të injektojë skripte keqdashëse që ekzekutohen në shfletuesit e përdoruesve të tjerë.

5. Cisco Evolved Programmable Network Manager (EPNM) dhe Cisco Prime Infrastructure – Open Redirect

- **CVE ID:** CVE-2026-20123
- **Rrezikshmëria:** Mesatare
- Një dobësi në ndërfaqet web të menaxhimit mund t'i lejojë një sulmuesi të paautentikuar nga distanca të ridrejtojë përdoruesit drejt faqeve keqdashëse për shkak të validimit të pasaktë të parametrave të kërkesave HTTP.

Rekomandime

AKSK rekomandon aplikimin e masave zbutëse të ofruara nga Cisco për produktet e prekura.

Referenca

https://sec.cloudapps.cisco.com/security/center/publicationListing.x