AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Përditësime të Sigurisë – Cisco

- CVE-2026-20034
- CVE-2026-20035
- CVE-2026-20185
- CVE-2026-20188
- CVE-2026-20167
- CVE-2026-20168
- CVE-2026-20169
- CVE-2026-20219
- CVE-2026-20189
- CVE-2026-20193
- CVE-2026-20195
- CVE-2026-20172
- CVE-2025-20204
- CVE-2025-20205

Data: 07/05/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Cisco ka publikuar përditësime sigurie për disa produkte të saj për të adresuar dobësi me rrezik të lartë dhe të mesëm. Këto dobësi mund të lejojnë ekzekutim kodi nga distanca, anashkalim autentikimi, sulme DoS, zbulim informacioni dhe sulme XSS. Organizatat që përdorin produktet e prekura rekomandohen të aplikojnë menjëherë përditësimet dhe masat zbutëse të ofruara nga Cisco.

Informacione Teknike

Dobësi me Rrezik të Lartë
• CVE-2026-20034, CVE-2026-20035 – Dobësi të Ekzekutimit të Kodit nga Distanca dhe Server-Side Request Forgery në Cisco Unity Connection
Dobësi që mund të lejojnë ekzekutimin e kodit arbitrar dhe Server-Side Request Forgery (SSRF) në Cisco Unity Connection.
• CVE-2026-20185 – Dobësi Denial of Service në Cisco SG350 dhe SG350X Series Managed Switches përmes SNMP
Dobësi që mund të shfrytëzohet për të shkaktuar ndërprerje të shërbimit (DoS) në switch-et e menaxhuara Cisco SG350 dhe SG350X.
• CVE-2026-20188 – Dobësi Connection Exhaustion Denial of Service në Cisco Crosswork Network Controller dhe Cisco Network Services Orchestrator
Dobësi që mund të lejojë konsumimin e lidhjeve dhe shkaktimin e sulmeve DoS.
• CVE-2026-20167, CVE-2026-20168, CVE-2026-20169 – Dobësi në Cisco IoT Field Network Director
Një grup dobësish që prekin Cisco IoT Field Network Director dhe mund të kompromentojnë funksionalitetin e sistemit.

Dobësi me Rrezik të Mesëm
• CVE-2026-20219 – Dobësi Insecure Direct Object Reference në Cisco Slido
Dobësi që mund të lejojë akses të paautorizuar në objekte ose të dhëna.
• CVE-2026-20189 – Dobësi Information Disclosure në Cisco Prime Infrastructure
Dobësi që mund të çojë në ekspozimin e informacionit sensitiv.
• CVE-2026-20193, CVE-2026-20195 – Dobësi Authentication Bypass në Cisco Identity Services Engine (ISE)
Dobësi që mund të lejojnë anashkalimin e mekanizmave të autentikimit.
• CVE-2026-20172 – Dobësi në Ngarkimin e Skedarëve në Cisco Enterprise Chat and Email Lite Agent
Dobësi që mund të lejojë ngarkimin e skedarëve keqdashës.
• CVE-2025-20204, CVE-2025-20205 – Stored Cross-Site Scripting (XSS) në Cisco Identity Services Engine

Dobësi Stored XSS që mund të përdoren për ekzekutimin e skripteve keqdashëse në aplikacion.

Rekomandime

AKSK rekomandon aplikimin e masave mitiguese ose workaround-eve të ofruara nga Cisco.

Referenca

- https://sec.cloudapps.cisco.com/security/center/publicationListing.x?utm_source=chatgpt.com