AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi në ekzekutimin e komandave në pikat e qasjes Wireless Hikvision

Data: 02/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Një dobësi me ashpërsi të lartë në disa produkte Hikvision Wireless Access Point mund të lejojë ekzekutimin arbitrar të komandave në pajisjet e prekura.

Informacione Teknike

Një dobësi në ekzekutimin e komandave është identifikuar në disa produkte të Hikvision Wireless Access Point. Problemi shkaktohet nga validimi i pamjaftueshëm i të dhënave hyrëse dhe u lejon sulmuesve të autentifikuar të ekzekutojnë komanda arbitrare në pajisjet e prekura. Shfrytëzimi i suksesshëm mund të rezultojë në kompromentim të plotë të pikës së aksesit dhe të ndikojë në konfidencialitetin, integritetin dhe disponueshmërinë e sistemit.

Detajet e dobësisë
• CVE-2026-0709
• Rezultati CVSS: 7.2 i Lartë
• Sulmuesit e autentifikuar me kredenciale të vlefshme mund ta shfrytëzojnë këtë dobësi duke dërguar paketa të krijuara posaçërisht që përmbajnë komanda keqdashëse, duke çuar në ekzekutimin arbitrar të komandave në sistemin operativ themelor.

Produktet e prekura
Modelet e mëposhtme të Hikvision Wireless Access Point preken kur ekzekutohet versioni V1.1.6303 build250812 ose më i hershëm:
• DS-3WAP521-SI
• DS-3WAP522-SI
• DS-3WAP621E-SI
• DS-3WAP622E-SI
• DS-3WAP623E-SI
• DS-3WAP622G-SI
Versione të përditësuara:
• V1.1.6601 build251223 ose më i ri

Rekomandime

AKSK rekomandon përditësimin e versioneve të prekura në versionet e rregulluara ose më të fundit të publikuara nga Hikvision.