AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi me Rrezikshmëri të Lartë në Pajisjet HP Poly Voice

Data: 03/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Është evidentuar një dobësi me rrezikshmëri të lartë në pajisjet HP Poly Voice që mund të lejojë imitimin e pajisjes dhe regjistrim të paautorizuar në shërbimet SIP.
Dobësia mund të lejojë imitimin e pajisjes nëse një çelës dhe certifikatë testimi të integruara nxirren përmes teknikave të specializuara të reverse engineering. Nëse ofruesit e shërbimeve nuk validonin siç duhet certifikatat e pajisjeve gjatë procesit të provisioning, pajisje të paautorizuara mund të regjistrohen në shërbimet SIP.

Informacione Teknike

Detaje të Dobësisë:

- **CVE ID:** CVE-2026-0754
- **CVSS Score:** 8.2 High

Dobësia ekziston për shkak të një çelësi dhe certifikate testimi të integruara brenda firmware-it të pajisjeve Poly Voice. Nëse këto kredenciale nxirren, ato mund të përdoren për të imituar pajisje legjitime gjatë lidhjes me mjedise ofruesish shërbimesh SIP që nuk zbatojnë validim të rreptë të certifikatave. Dobësia prek kryesisht proceset e provisioning dhe autentikimit, jo komunikimet direkte pajisje-me-pajisje.

Shfrytëzimi me sukses mund t'u lejojë sulmuesve të:

- Imitojnë endpoint-e legjitime SIP
- Regjistrojnë pajisje të paautorizuara në shërbimet SIP
- Aksesojnë ose përgjojnë sesione komunikimi
- Shkaktojnë ndërprerje shërbimi në infrastrukturat e zërit

Produktet e Prekura dhe Versionet e Rregulluara

Emri i Produktit	Versioni i Rregulluar
VVX	UCS 6.4.8
Edge E	PVOS 8.5.0
Trio 8300	UCS 8.1.7.c

Rekomandime

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

Referenca

https://support.hp.com/us-en/document/ish_14269649-14269682-16/hpsbpy04081