



AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Dobësi me ashpërsi të lartë në HPE Aruba Private 5G Core On-Prem

Data: 09/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive	2
Informacione Teknike	2
Rekomandime	2

Përmbledhje Ekzekutive

Një dobësi e ridrejtimin të hapur me ashpërsi të lartë në platformën HPE Aruba Networking Private 5G Core On-Prem. Dobësia ekziston në rrjedhën e hyrjes në GUI dhe mund t'u lejojë sulmuesve të ridrejtojnë përdoruesit në faqet e internetit keqdashëse, duke çuar potencialisht në kompromentimin e kredencialeve dhe akses të paautorizuar.

Informacione Teknike

- ID e CVE: CVE-2026-23818
- Ashpërsia: E lartë Rezultati i CVSS v3.1: 8.8
- Dobësia shkaktohet nga validimi i papërshtatshëm i të dhënave të kontrolluara nga përdoruesi brenda procesit të hyrjes në ndërfaqen grafike të përdoruesit (GUI), duke çuar në një gjendje të hapur ridrejtimi.
- Një sulmues mund të krijojë një URL dashakeqe që ridrejton një përdorues legjitim në një faqe interneti të kontrolluar nga sulmuesi. Kjo faqe mund të imitojë faqen legjitime të hyrjes për të mashtruar përdoruesit që të futin kredencialet e tyre. Pasi të kapet, përdoruesi mund të ridrejtohet përsëri në aplikacionin origjinal, duke e bërë sulmin më pak të dukshëm.

Ndikimi

- Mbledhja e kredencialeve nëpërmjet phishing
- Qasje e paautorizuar në sisteme
- Skenarë të mundshëm anashkalimi të vërtetimit
- Ekspozimi ndaj sulmeve dashakeqe të ridrejtimin

Versionet e prekura

- HPE Aruba Networking Private 5G Core On-Prem Versionet 1.25.3.0 dhe më të ulëta

Versionet e përditësuar

- HPE Aruba Networking Private 5G Core 1.25.3.1 dhe më të reja

Rekomandime

AKSK rekomandon zbatimin e zbutjes ose zgjidhjes alternative të ofruar nga HPE Aruba Networking.