EXECUTIVE BRIEF

Digital infrastructure and operational risk

Case Study: The Medina of Fez, Morocco

TLP:CLEAR · Author: Rob Pinna · robpinna.com

Field: 3–6 March 2026 · OSINT: Jan–Mar 2026

BOTTOM LINE UP FRONT

Commercial assets in the Medina of Fez operate inside a structurally exposed digital environment. Two independent layers are present: internet-facing surveillance infrastructure reachable from the public internet, and a dense informal wireless layer with near-universal WPS enablement and zero enterprise-grade posture. Where the two converge on flat, unsegmented networks, the combined exposure surface creates conditions that would support passive collection, credential exposure and lateral access by any actor with physical proximity and basic technical capability. The structural exposure is assessed at HIGH confidence. Attribution to specific actor categories is not asserted from passive collection alone.

Layer 1: 3,890 surveillance-related endpoints reachable from the public internet across the Fez metropolitan area, with an estimated 500 to 1,100 inside the Medina. Layer 2: along the three principal tourist arteries of Fes el-Bali, 1,027 unique BSSIDs, 76.3% with WPS enabled, zero enterprise-grade.

Methodology

Hybrid collection combining passive OSINT enumeration of internet-facing surveillance infrastructure (Shodan, Censys; ASN-filtered to Maroc Telecom AS6713) with on-the-ground passive Wi-Fi proximity collection along Tala'a Sghira, Tala'a Kebira, and the Bab Rcif corridor (WiGLE methodology, deduplicated by BSSID). No active probing, authentication attempts, or interception of any kind. Findings reported under ICD-203 estimative-language conventions with explicit confidence tiering.

Key Findings

- **Scale (Layer 1, OSINT).** 3,890 surveillance-related endpoints across the Fez metropolitan area; estimated 500 to 1,100 concentrated in the Medina (scenario-derived, MODERATE confidence).
- **Local network posture (Layer 2, field).** Of 1,027 unique BSSIDs in the corridor sample: 76.3% WPS-enabled, 72.1% legacy 2.4 GHz only, 0% enterprise-grade, 0% Wi-Fi 6E.
- **Hardware homogeneity.** Arcadyan equipment (Maroc Telecom ISP-issued routers) accounts for 33.7% of the corridor sample, the largest single vendor share. The hardware baseline is homogeneous and consumer-grade throughout.
- **Vulnerability landscape.** Among endpoints exposing firmware metadata (n=429), 56.9% sit in the 2018–2020 generation, the cohort with the highest density of publicly disclosed CVEs for Hikvision and Dahua platforms (incl. CVE-2021-36260, CVE-2021-33044/45, all CVSS ≥ 9.8).

What this assessment does and does not claim

Findings represent structural feasibility, not incident confirmation. The Wi-Fi survey is a convenience sample of the three named tourist corridors, not a census of the Medina. CVE references describe vulnerabilities in the device families dominant in this environment; they are not asserted as confirmed on individual endpoints. Confidence: HIGH on structural exposure, MODERATE on Medina concentration estimates, LOW on attribution.

Full report (v3.9, 19 pp): robpinna.com · Includes hybrid exposure model, threat-actor reference frame, MITRE ATT&CK mapping, key risk indicators, operational scenarios, and full source list.

About the author. Roberto Pinna is an independent digital risk intelligence analyst with thirteen years of recurring field work in Morocco. CompTIA Security+, EC-Council Certified Threat Intelligence Analyst (CTIA). Published research at robpinna.com.

direct@robpinna.com · linkedin.com/in/pinnarob · robpinna.com