**Document**

| | |
|---|---|
| Classification: | TLP;CLEAR. Unrestricted. |
| Version: | 3.9 (revised, April 2026) |
| Collection window: | January 2026 – March 2026 |
| Author: | Roberto Pinna |
| Client: | |

**Handling caveat**

Findings represent structural feasibility, not incident confirmation. No active exploitation, credential testing, or network access of any kind was conducted. Data sourced exclusively from passive, publicly accessible platforms and ground-level observation in public space.

# Digital Infrastructure and Operational Risk

*Assessment of remote and local cyber exposure, informal connectivity, and inherited risk for investors and operators in the Medina of Fez, Morocco.*



Private assessment


direct@robpinna.com
www.robpinna.com

Italy
Cagliari

Morocco
Fez / Marrakech

+39
3426988107

# 1. Bottom Line Up Front

Commercial assets in the Medina of Fez sit inside an exposure environment consistent with the tradecraft of criminal access brokers, fraud operators, and intelligence-adjacent collectors operating at low footprint. Two independent layers are present: remotely reachable surveillance infrastructure (Layer 1) and an informal, trust-based local wireless environment (Layer 2). Where the two meet on flat unsegmented networks, the combined attack surface is worse than either in isolation.

The numbers: 3,890 surveillance-related endpoints reachable from the public internet across the Fez metropolitan area, with an estimated 500 to 1,100 in the Medina. On the ground along the three main tourist arteries of Fes el-Bali, a four-day passive Wi-Fi survey detected 1,027 unique BSSIDs, of which 76.3% had WPS enabled, a known vulnerability that requires nothing more than commodity software and physical proximity. Zero enterprise-grade deployments across the entire corridor sample.

Published CVEs for the camera and NVR platforms dominant in this environment (Hikvision, Dahua) include authentication bypass and unauthenticated command injection. WPS PIN cracking tools (Reaver, Bully) cover Layer 2 access.

The risk profile fits the tradecraft of criminal access brokers, fraud operators, and intelligence-adjacent collectors prioritising persistence and data collection over disruption. As Morocco's commercial profile rises with the 2030 World Cup and Casablanca Finance City, the value of that access increases.

Confidence is HIGH on structural exposure, MODERATE on Medina concentration estimates, and LOW on attribution without victim-side telemetry.

# 2. Executive Summary

The Medina of Fez presents a Hybrid Exposure Model: informal, trust-based digital networks intersecting with legacy internet-facing surveillance infrastructure in ways that standard perimeter-based security models do not address.

In dense urban environments across the MENA region, digital infrastructure tends to be informal: Wi-Fi passwords are shared between neighbours, surveillance footage is exchanged on request, router access passes through family or trade networks. This is not a failure of awareness, it is how things work. It also creates a network environment that is laterally permeable in ways perimeter-based security models do not address.

Passive OSINT enumeration identified 3,890 unique surveillance-related endpoints across the Fez metropolitan area, with an estimated 500 to 1,100 concentrated in the Medina. A ground-level Wi-Fi proximity survey conducted along the three principal tourist arteries of Fes el-Bali (Tala'a Sghira, Tala'a Kebira, and the Bab Rcif corridor) detected 1,027 unique BSSIDs after removing duplicate observations across multiple passes. Of these, 76.3% were WPS-enabled, 72.1% operated on the legacy 2.4 GHz band exclusively, and 0% were enterprise-grade. No Wi-Fi 6E infrastructure was observed. The two empirical layers operate at different geographic scopes: the remote OSINT layer is city-level, the field layer is a corridor sample within Fes el-Bali.

Of the surveillance endpoints exposing firmware metadata (n=429, 11.0% of the enumerated dataset), the majority belong to the 2018 to 2020 firmware generation, a cohort carrying the highest density of publicly disclosed, unpatched CVEs for these vendor families.

This risk profile is consistent with tradecraft typically associated with criminal access brokers, fraud operators, and intelligence-adjacent collectors prioritising persistent, low-footprint access and data monetisation over

disruption. As Morocco attracts international investment, these dynamics introduce non-obvious risks for foreign market entrants.

## 3. Analytical Standards

This assessment follows estimative language conventions consistent with Intelligence Community Directive 203 (ICD-203). Verbal probability terms map to the following approximate ranges:

| Verbal Term | Approximate Probability Range |
|---|---|
| Almost certain | Greater than 95% |
| Highly likely | 80 to 95% |
| Likely | 55 to 80% |
| Roughly even | 45 to 55% |
| Unlikely | 20 to 45% |
| Highly unlikely | 5 to 20% |
| Remote | Less than 5% |

Source confidence levels in Key Judgements use a three-tier scheme:

- **HIGH.** Strong evidential basis from direct observation or well-established technical documentation. Low inferential dependency.
- **MODERATE.** Structural plausibility supported by partial evidence. Requires additional collection to confirm.
- **LOW.** Analytically derived from first principles or analogical reasoning. Speculative pending additional data.

This document assesses exposure feasibility, not confirmed compromise. Probability statements refer to the likelihood that structural conditions are exploitable, not that exploitation has occurred.

## 4. Strategic Context: Morocco

Morocco is among the MENA region's most active investment frontiers. The kingdom co-hosts the 2030 FIFA World Cup, which is catalysing infrastructure development and tourism expansion. Casablanca Finance City positions Morocco as a continental financial hub. The Tangier-Med industrial zone embeds Morocco in European automotive supply chains. These dynamics concentrate commercially valuable human and business intelligence in urban centres including Fez, the kingdom's historic cultural capital and a growing destination for heritage tourism investment.

### Regulatory Environment

Morocco's cybersecurity and data governance framework is established but uneven in enforcement. The DGSSI is the national cybersecurity authority, with maCERT operating beneath it as the national CERT. The CNDP supervises personal data protection under Law 09-08 (2009), and Law 05-20 (2020) sets the national cybersecurity framework, defining critical infrastructure obligations and incident notification duties. The gap

between regulatory intent and enforcement at the micro-business level is a structural condition rather than a policy failure, reflecting resource allocation realities common to most emerging markets.

**Assessment relevance.** Investment acceleration increases the value of contextual identity and business intelligence observable from within these environments. The risk is likely to intensify before regulatory capacity scales to match it.

# 5. Methodology and Data Sources

### Scope

This assessment focuses on civilian camera and surveillance infrastructure and associated network exposure within the Medina of Fez, Morocco. It explicitly excludes active probing, authentication attempts, exploitation, credential testing, vulnerability scanning, or interception of any kind. No unauthorised network access was sought or achieved.

### Data Sources

#### *Remote OSINT Enumeration*

Passive enumeration of internet-facing assets using Shodan and Censys. Representative query patterns targeted:

- RTSP-exposed endpoints (port 554) attributed to Fez-area IP ranges
- HTTP/HTTPS administration interfaces on ports 80, 443, 8080, 8443
- Device banner strings and firmware metadata associated with IP camera and NVR product families (Hikvision, Dahua, XiongMai-based platforms)
- ISP-level ASN filtering, with Maroc Telecom AS6713 as primary

Results from multiple queries were merged into a single dataset and deduplicated using IP address plus port as a composite key. Internet-facing assets are treated as a proxy for broader, partially observable exposure. NAT-based shared networks mean actual device counts are likely higher than enumerated.

#### *Field Survey (Wi-Fi Proximity)*

A passive Wi-Fi proximity survey was conducted from 3 to 6 March 2026, using WiGLE wardriving methodology. The survey covered three principal tourist arteries within Fes el-Bali (the historic Medina): Tala'a Sghira and Tala'a Kebira, both originating at the Bab Boujloud main entrance, and the corridor leading to the Bab Rcif gate. These three axes carry the bulk of the Medina's tourist foot traffic and concentrate most riad accommodations and tourism-facing commerce, making them the segment where the documented exposure model is most directly relevant to the report's commercial audience.

***Scope and sampling note.*** *The Wi-Fi survey is a convenience sample of the three corridors named above. It is not a census of the Medina. Generalisation to residential interior areas of Fes el-Bali or to Fes el-Jdid would require additional sampling.*

Data collection was passive: no probe-request injection, network association, or traffic interception. The survey was conducted in public space in compliance with applicable Moroccan law.

**Deduplication protocol.** WiGLE logs each detected access point on every pass through its proximity range. Across four days of overlapping coverage, the same BSSID was frequently recorded multiple times. The dataset was deduplicated by collapsing repeated observations into a single record per unique hardware identifier. The figure of 1,027 unique BSSIDs reflects this deduplication; the pre-deduplication observation count was 3,210.

No SSID names, MAC addresses, or device-level geolocation data are retained or reported. Vendor attribution is based solely on OUI prefix analysis applied to anonymised hardware identifiers. Results are reported as BSSIDs throughout. A BSSID corresponds to a single radio interface; dual-band hardware emits two BSSIDs (2.4 GHz and 5 GHz), so the number of physical access points is at or below the BSSID count. The 72.1% single-band rate implies that a majority of physical devices in the sample are single-band, but the BSSID figure is used as the analytical denominator throughout for consistency.

#### *Secondary Sources*

Open demographic data, Moroccan urban density references, secondary OSINT on tourism density and Medina spatial structure, publicly disclosed CVE databases (NIST NVD), and published academic and security research on WPS vulnerabilities and consumer surveillance infrastructure.

### Limitations

- City-level geolocation in Shodan and Censys limits neighbourhood-level precision. Medina concentration estimates are scenario-derived (Section 9).
- NAT-based shared networks cause significant under-representation. Many devices sit behind a single public IP.
- Single observation window prevents longitudinal trend analysis.
- The two empirical layers operate at different geographic scopes: the remote OSINT layer covers the Fez metropolitan area, the Wi-Fi survey covers a defined corridor sample within Fes el-Bali. The datasets are not co-extensive and are not used as cross-validations of the same population.
- Findings represent structural feasibility, not incident confirmation. No victim-side telemetry was available.
- WPS-enabled status is observable passively. Actual exploitability depends on router model and firmware configuration.

## 6. OSINT Findings: Scale and Distribution

### Key Metrics

| Figure | Description |
|---|---|
| 3,890 | Unique surveillance-related endpoints identified across the Fez metropolitan area (deduplicated by IP + port composite key). City-level scope. |
| 500 to 1,100 | Estimated endpoints plausibly concentrated in the Medina (scenario-based, see Section 9). |
| 1,027 | Unique BSSIDs detected along the three principal tourist arteries of Fes el-Bali (Tala'a Sghira, Tala'a Kebira, the Bab Rcif corridor) over four days of passive wardriving in March 2026, after deduplication. Tourist-corridor scope. |
| 3,210 | Pre-deduplication WiGLE observation count for the same corridor sample, retained for methodological transparency. |
| 429 | Endpoints exposing sufficient firmware metadata for version classification (11.0% of the Fez-wide enumerated dataset). |

### Surveillance Endpoint Composition

Identified surveillance-related endpoints include:

- RTSP-exposed streams on port 554 (primary enumeration target)
- HTTP/HTTPS administration interfaces on ports 80, 443, 8080, 8443
- Cloud P2P relay registrations observable via banner metadata
- NVR systems with combined port exposure in the 8000 to 8999 range

Banner analysis of versioned endpoints is consistent with the regional deployment profile in MENA markets, dominated by Hikvision and Dahua, which determines the CVE families applicable in Section 7.

### Legacy Firmware Indicators

Of the 429 endpoints that exposed firmware version metadata (11.0% of the 3,890-endpoint dataset), the age distribution is as follows:

| Firmware Generation | Observed Count | Share of Versioned Subset (n=429) | Share of Total (n=3,890) |
|---|---|---|---|
| 2014 to 2017 | 51 | 11.9% | 1.3% |
| 2018 to 2020 | 244 | 56.9% | 6.3% |
| 2021 to Present | 134 | 31.2% | 3.4% |
| Total versioned | 429 | 100.0% | 11.0% |
| No version metadata | 3,461 | n/a | 89.0% |

The majority of endpoints (89.0%) do not expose firmware version metadata. This does not indicate modern firmware. It more commonly reflects configuration defaults that suppress banner disclosure. The versioned subset (n=429) is therefore not a random sample of the full dataset: it over-represents devices whose administrators have not suppressed banner output, which may not be uniformly distributed across firmware generations or operator types. Findings from this subset should be read as indicative of the vulnerability landscape, not as a statistically representative breakdown of the full 3,890-endpoint population. With that caveat, the 2018 to 2020 cohort, which accounts for 56.9% of versioned endpoints, corresponds to a generation of Hikvision, Dahua, and XiongMai-based platforms with the highest density of publicly disclosed, unpatched CVEs (see Section 7).

Older firmware here is not negligence. Devices stay in place because they still work, and replacement is expensive in a micro-business economy. The risk implication is structural, not a fault of the operators.

## 7. Technical Vulnerability Profile

OSINT metadata indicates continued presence of legacy camera and NVR platforms with publicly disclosed, unpatched vulnerabilities. The CVEs below are directly relevant to the device families identified in this assessment. All identifiers are drawn from the NIST National Vulnerability Database (NVD) and are verifiable via public sources.

***Note on scope of CVE citation.*** *These CVEs describe publicly known vulnerabilities in the device families dominant in this environment. They are not asserted as confirmed on individual endpoints: passive OSINT enumeration*

*does not permit model-level or firmware-level verification. The argument is structural—the combination of Hikvision/Dahua prevalence and the legacy firmware cohort (56.9% of versioned endpoints in the 2018–2020 generation, see Section 6) creates conditions in which vulnerabilities of this class are statistically likely to be present across a material portion of the exposed population.*

| CVE | Vendor | CVSS | Description |
|---|---|---|---|
| CVE-2017-7921 | Hikvision | 8.8 | Authentication bypass via specially crafted URL parameters, allowing unauthenticated access to device functions. Hardcoded credentials also present in affected firmware versions. |
| CVE-2021-36260 | Hikvision | 9.8 (Critical) | Unauthenticated command injection via the web server component. Exploitable remotely with no prior authentication. Enables full device takeover. |
| CVE-2021-33044 | Dahua | 9.8 (Critical) | Authentication bypass in Dahua IP cameras and NVR platforms (the Magic Packet bypass). Allows unauthenticated access to administrative functions. |
| CVE-2021-33045 | Dahua | 9.8 (Critical) | Authentication bypass variant affecting a broader range of Dahua camera and NVR models. Related to CVE-2021-33044, distinct in affected code path. |

### WPS Protocol Vulnerability (Non-CVE)

WPS PIN-based authentication (Wi-Fi Protected Setup) is subject to an inherent design flaw first documented by Stefan Viehboeck in 2011, with independent concurrent discovery by Craig Heffner. The flaw allows the 8-digit PIN to be brute-forced in two sequential 4-digit segments, reducing the effective keyspace from 10^8 to approximately 11,000 guesses. This is not assigned a CVE because it is a protocol design flaw, not an implementation bug.

Commodity toolkits implementing this attack, including Reaver and Bully, are freely available, require minimal technical skill, and operate without prior network credentials until the PIN is recovered. With 76.3% of surveyed BSSIDs WPS-enabled (see Section 8), this constitutes the primary low-skill access vector for Layer 2.

### Operational Significance

The combination of Layer 1 CVEs and the Layer 2 WPS protocol flaw may enable persistent access to both surveillance streams and local network segments without triggering authentication-based detection, where the relevant device or network configuration remains vulnerable. Neither attack pathway requires interaction with a human operator or escalation of privilege beyond initial access.

## 8. Network Security Profile: Wi-Fi Proximity Survey

A passive Wi-Fi proximity survey was conducted along the three principal tourist arteries of Fes el-Bali (Tala'a Sghira, Tala'a Kebira, and the corridor leading to Bab Rcif) using WiGLE wardriving methodology (3 to 6 March 2026). After deduplication of repeat observations across multiple passes along the same corridors, the survey identified 1,027 unique BSSIDs. The pre-deduplication raw observation count was 3,210. This figure is retained in this assessment for methodological transparency but is not used as the analytical denominator. All percentages in this section are calculated against the 1,027 deduplicated BSSID baseline.

***Scope.*** *Findings describe the wireless environment of the three named tourist corridors, not of the entire Medina (Section 5).*

### Hardware Composition

OUI-based vendor identification reveals Arcadyan Technology equipment as the largest single vendor share in the corridor sample (33.7% of the 1,027 BSSIDs), the manufacturer of the standard ISP-provisioned routers distributed by Maroc Telecom. Within the surveyed corridors, this indicates a homogeneous, ISP-managed hardware baseline among a plurality of devices, a finding consistent with Maroc Telecom's dominant market position in Fez. The pattern is expected to extend to other parts of the Medina but has not been empirically confirmed outside the corridor sample.

Consumer-grade router homogeneity has two analytical implications. First, it reduces the variance in security posture: what is true of one router type is likely true of most. Second, it creates conditions where a single ISP firmware vulnerability could have area-wide impact in commercially relevant zones.

### Network Security Profile Table

| Security Indicator | Count | Share of n=1,027 |
|---|---|---|
| WPS-enabled (all APs) | 784 | 76.3% |
| Mixed WPA/WPA2 mode (legacy compatibility) | 266 | 25.9% |
| Open or unencrypted networks | 24 | 2.3% |
| 2.4 GHz band only (legacy hardware) | 740 | 72.1% |
| Wi-Fi 6E (6 GHz band, modern) | 0 | 0.0% |
| Enterprise-grade (WPA2/3-Enterprise) | 0 | 0.0% |

### Operationally Significant Findings

- **WPS prevalence (76.3%).** The most significant finding. With 784 of 1,027 BSSIDs WPS-enabled, the Viehboeck/Heffner PIN brute-force attack is feasible against the majority of surveyed infrastructure without prior knowledge of network credentials.
- **Zero enterprise-grade deployments.** The complete absence of WPA2/3-Enterprise (802.1X/RADIUS-based authentication) confirms that the surveyed wireless infrastructure is entirely consumer-grade. There is no per-user authentication, no certificate-based access control, and no centralised session management anywhere in the surveyed corridors.
- **Legacy band dominance (72.1% on 2.4 GHz only).** Consistent with entry-level or legacy consumer hardware without dual-band capability. The absence of Wi-Fi 6E in the corridor sample is consistent with no infrastructure refresh at scale in the surveyed zones.
- **Open networks (2.3%).** While numerically small, 24 open networks within the corridor sample represent zero-friction access points for passive traffic observation.

### Local Layer: Operational Profile

These findings provide empirical evidence for the Layer 2 component of the Hybrid Exposure Model in the corridors most relevant to tourism-facing operators and investors. The wireless infrastructure carrying

commercial traffic along these corridors is overwhelmingly the kind of off-the-shelf household equipment found in any home, with WPS enabled, legacy hardware, and no enterprise authentication anywhere.

The same pattern is expected to extend to other parts of the Medina, given the dominance of Maroc Telecom's ISP-provisioned hardware across Fez. That extension is not empirically confirmed by this collection cycle and is not claimed here.

## 9. Estimation Model: Medina Focus

This section addresses Layer 1 only (the surveillance infrastructure reachable from the public internet). The Wi-Fi survey in Section 8 has its own scope (the three tourist arteries of Fes el-Bali) and is not the empirical basis for this estimation.

City-level geolocation in Shodan and Censys assigns coordinates at ISP POP or city centroid level, not device level. A scenario-based estimation was applied to derive plausible surveillance endpoint concentration within the Medina specifically.

### Estimation Assumptions

The Medina represents approximately 8 to 9% of Fez's total population (around 90,000 to 100,000 of 1.1 million residents, per Moroccan census-adjacent urban planning data). Tourism-facing micro-business density in the Medina substantially exceeds the city average, concentrating most riad accommodations, artisan workshops, and hospitality venues. Surveillance density correlates with foot traffic, access control needs, and property value per square metre, all elevated in the Medina relative to surrounding districts. Comparable heritage tourism zones (Marrakech, Tunis) show similar patterns.

### Scenario Range

| Scenario | Estimate | Logic | Confidence |
|---|---|---|---|
| Conservative | ~500 endpoints | Medina share proportional to population (~8-9% of 3,890 = ~320-355), adjusted upward for commercial density. | HIGH |
| Realistic | ~600 to 750 endpoints | Applies a 1.8 to 2.2x density multiplier over population-proportional baseline to reflect commercial concentration. | MODERATE |
| Stress | ~1,100 endpoints | Assumes Medina disproportionately concentrates online surveillance given tourism investment density (~28% of city total). | LOW |

These are scenario-derived estimates, not empirically confirmed counts. Calibration of the realistic-range multiplier (1.8 to 2.2x over population-proportional baseline) is informed by field observation of tourism-density patterns across Moroccan medinas, not by quantitative cross-validation between the OSINT and Wi-Fi datasets. The two datasets describe different layers of the model and operate at different scopes (Section 6).

## 10. Hybrid Exposure Model

The exposure conditions documented in Sections 6 and 8 form a repeatable hybrid model. The dominant risk dynamic arises from the interaction of two distinct layers, which together create compounded exposure greater than either layer in isolation.

### Layer 1: Internet-Facing (Remote Access)

Layer 1 is exploitable from anywhere. An attacker with OSINT access and commodity tooling does not need to be in Fez to exercise it.

- **Attack surface.** Legacy CCTV/NVR systems (RTSP ports 554, 8000 to 8999); administration interfaces (HTTP/HTTPS on 80, 443, 8080, 8443); cloud relay services (P2P protocols enabling remote access via manufacturer cloud, bypassing NAT).
- **Primary vulnerabilities.** Authentication bypass and remote code execution of the class documented in Section 7, alongside default-credential exposure documented industry-wide for these vendor families.
- **Attacker capability requirement.** LOW to MODERATE. Detection difficulty for defenders: HIGH (no authentication event generated in bypass exploitation).

### Layer 2: Local Shared Network (Proximity Access)

Layer 2 needs someone physically present, with a useful working radius of roughly 50 to 150 metres in dense urban fabric. That person could be a tourist, a vendor, a neighbour, or someone working there on purpose.

- **Attack surface.** Consumer-grade guest Wi-Fi environments in the surveyed corridors, with no observed enterprise authentication and high WPS prevalence (784 of 1,027 BSSIDs, 76.3%). The absence of enterprise-grade deployments is consistent with weak segmentation practices, but property-level confirmation that guest Wi-Fi, surveillance, POS, and management devices share the same subnet would require site inspection (see Section 16, PIR-2).
- **Primary attack vector.** WPS PIN brute-force via Reaver or Bully. Attacker capability requirement: LOW (commodity toolkit, minimal skill). Time to access: variable, typically hours to days for WPS PIN recovery. Detection difficulty for defenders: HIGH (brute-force generates no authentication success events until completion, producing minimal alertable anomaly on consumer-grade equipment).

### Compounded Exposure

Where Layer 1 and Layer 2 conditions co-exist, as they do in properties where remotely reachable cameras and guest Wi-Fi share one flat network, the effective attack surface includes both remote access to surveillance streams and local network traversal from a single initial access event. With no segmentation, lateral movement between surveillance, commercial, and guest traffic is structurally unrestricted once a foothold is established at either layer. Standard perimeter monitoring has no surface to work against.

## 11. Threat Actor Reference Frame

The archetypes below describe adversaries whose tradecraft fits the conditions documented above. They are reference profiles drawn from publicly documented tradecraft in comparable environments, not assertions of confirmed activity here.

| Actor Archetype | Plausible Objective | Conditions That Would Enable Access |
|---|---|---|
| Criminal Access Brokers | Acquire and resell footholds tied to commercially useful environments. Build access inventory for downstream clients (fraud operators, competitors, collectors). | RTSP/NVR exposure of the class documented in Section 7; weakly segmented guest Wi-Fi; WPS-enabled local access surface (Section 8). |
| Financially Motivated Fraud Operators | Build high-credibility fraud using contextual identity fragments (tourism fraud, fake rental listings, impersonation schemes). | Surveillance stream observability; local network traffic capture on flat topology; business identity aggregation from publicly visible signage and exposed devices. |
| Intelligence-Adjacent Collectors | Maintain low-noise visibility on people, patterns, and places of interest. Pattern-of-life profiling. | Persistent remote RTSP observation; proximity-based shared network access for enhanced targeting in the documented environment. |

## 12. MITRE ATT&CK Reference Frame for Defenders

***Important framing.*** *Techniques mapped below are those an adversary would exercise against the documented conditions. They are provided as a defender reference frame, not as a record of observed activity.*

Techniques are organised below by MITRE ATT&CK tactic, reflecting the order in which a hypothetical adversary would progress through the kill chain against the documented conditions. Technique IDs reference MITRE ATT&CK and can be verified at attack.mitre.org.

| Tactic | ID | Technique | Why It Would Apply Here |
|---|---|---|---|
| Reconnaissance | T1589 | Gather Victim Identity Information | An adversary could aggregate identity fragments (faces, routines, business names, signage) observable from surveillance streams and publicly visible commercial environments documented in this report. |
| Reconnaissance | T1590 | Gather Victim Network Information | Public OSINT enumeration via Shodan and Censys, of the type used in Section 5, would surface the same exposure documented here. |
| Initial Access | T1190 | Exploit Public-Facing Application | Would apply to exploitation of CVEs in the class documented in Section 7, against internet-exposed camera and NVR administration interfaces. |
| Initial Access | T1133 | External Remote Services | Would apply to abuse of RTSP streams and vendor cloud P2P relay services as remote access channels. |
| Initial Access | T1078 | Valid Accounts | Would apply to the use of hardcoded or default credentials documented in the public CVE record for vendor families dominant in the surveyed environment. |

| Tactic | ID | Technique | Why It Would Apply Here |
|---|---|---|---|
| Credential Access | T1110 | Brute Force | Would apply to WPS PIN brute-force (Viehboeck/Heffner methodology) against the WPS-enabled access points documented in Section 8 (76.3% of the surveyed BSSIDs). |
| Discovery | T1046 | Network Service Discovery | Would apply to mapping of services on flat guest/surveillance subnets, given the absence of segmentation documented in the surveyed environment. |
| Discovery | T1018 | Remote System Discovery | Would apply to enumeration of devices on flat shared subnets following initial access at either layer. |
| Collection | T1125 | Video Capture | Would apply to persistent observation of surveillance streams enabling pattern-of-life analysis. |
| Collection | T1040 | Network Sniffing | Would apply to passive traffic capture on flat consumer networks. |
| Command and Control | T1071.001 | Application Layer Protocol: Web Protocols | Would apply to use of HTTP/RTSP for command and control or exfiltration, blending with legitimate surveillance traffic. |

## 13. Key Judgements

| # | Judgement | Confidence |
|---|---|---|
| J1 | Trust-based shared infrastructure is structurally embedded in dense urban environments. The proximity survey confirms scale and exclusively consumer-grade hardware profile in the principal tourist corridors of Fes el-Bali, with the same pattern expected, though not empirically confirmed by this collection cycle, in adjacent Medina areas. | HIGH |
| J2 | Observable OSINT exposure is a lower bound of total risk surface. The remote enumeration documents the city-level Layer 1; the corridor-level Wi-Fi survey documents a Layer 2 not reachable by remote collection. The two layers operate at different geographic scopes and together describe a hybrid exposure profile. | HIGH |
| J3 | Concentration of surveillance endpoints in the Medina is plausible under density-adjusted scenario modelling. | MODERATE |
| J4 | Hybrid exposure (Layer 1 plus Layer 2 combined) amplifies feasibility of passive exploitation without requiring elevated attacker capability. | HIGH |
| J5 | Identity aggregation from surveillance and shared network access is feasible without overt intrusion or network disruption. | MODERATE |
| J6 | The structural conditions are consistent with tradecraft of actors who would prioritise persistence, observation, and monetisation over disruptive or noisy operations, if such actors were active in this environment. | MODERATE |

| # | Judgement | Confidence |
|---|---|---|
| J7 | Long-term low-footprint abuse is unlikely to be detected by local operators without deliberate monitoring tooling. | HIGH |
| J8 | Risk exposure is likely to increase alongside economic growth, driven by digitalisation of micro-businesses, persistence of legacy infrastructure, and rising value of contextual identity in a higher-investment environment. | HIGH |

***Analytical note.*** *The primary risk here is not disruptive intrusion. It is durable, low-noise access that supports observation and identity enrichment for downstream monetisation. Standard incident detection assumptions do not apply.*

## 14. Operational Scenarios

***Framing.*** *The following scenarios describe how an adversary could exploit the documented conditions, not how an adversary is doing so. They are analytical constructs intended to support risk reasoning.*

### Scenario 1: Identity Harvesting for High-Credibility Fraud

An actor with access to persistent RTSP streams from multiple riads and guesthouses could aggregate identity fragments over time: faces, routines, vehicle registrations, business logos, phone numbers displayed on signage, and check-in patterns. This data could enrich synthetic profiles or fraudulent tourism listings (such as Airbnb or Booking.com clones) with locally authentic detail, including photographs of real properties, business names with verifiable online presence, and plausible operator identities, sufficient to deceive foreign visitors and investors. Confidence in structural feasibility: MODERATE-HIGH.

### Scenario 2: Contextualised Access Brokerage

Footholds tied to identifiable commercial clusters, including riads, guesthouses, and craft workshops, could be enumerated, validated, and resold to downstream actors via access broker markets. The commercial context of the access (known hospitality or tourism-adjacent infrastructure) would command a premium over generic undifferentiated device access. Confidence in structural feasibility: MODERATE.

### Scenario 3: Supply Chain Intelligence for Market Entrants

A foreign investor conducting due diligence on a riad acquisition or hospitality franchise opportunity could operate within a flat-network environment without awareness of shared surveillance or network exposure. Documents, financial discussions, and communication patterns observable on guest networks or through accessible surveillance streams could in principle inform competing bids or negotiation positioning. Confidence in structural feasibility: LOW-MODERATE (would require an adversary with prior knowledge of investor presence and access to relevant infrastructure).

## 15. Key Risk Indicators and Early Warning Signals

Indicators are selected for observability and trend sensitivity rather than precision attribution. They are appropriate for periodic monitoring by analysts maintaining situational awareness on this environment.

### Key Risk Indicators (KRIs): Monitor for Trend Change

- **Volume of RTSP-exposed endpoints (Shodan/Censys repeat queries).** Baseline 3,890 (January to March 2026). Growth indicates expanding attack surface; decline may indicate ISP-level remediation or NAT migration.
- **Persistence of 2018 to 2020 firmware generation cohort (currently 56.9% of versioned subset).** Decline indicates upgrade activity; persistence into 2027 increases CVE-relevant exposure window.
- **ISP router vendor concentration (Arcadyan/Maroc Telecom 33.7% in the March 2026 corridor sample).** Shift in vendor distribution may indicate ISP CPE refresh program.
- **WPS-enabled BSSID prevalence (baseline 76.3% in the Fes el-Bali tourist corridor sample, March 2026).** Monitored via future wardriving collection windows, ideally with expanded sampling beyond the original three corridors. Decline below 50% would indicate meaningful security improvement in the local layer of the surveyed zones.
- **Wi-Fi 6E (6 GHz band) deployment (currently 0%).** Emergence would indicate infrastructure modernisation. Wi-Fi 6E does not support WPS by default.

### Early Warning Signals (EWS): Possible Indicators of Active Abuse

- Surge in fraudulent tourism listings using authentic local photography, real business names, or verifiable venue identities.
- Recycled business identifiers (phone numbers, registered trade names, visual branding) appearing in impersonation campaigns targeting international visitors or investors.
- Social engineering attempts against foreign visitors or investors that demonstrate local contextual knowledge inconsistent with publicly available information (suggests surveillance-derived intelligence).
- Access resale activity on criminal marketplaces referencing Moroccan hospitality or tourism infrastructure (monitor relevant dark web communities and broker forum categories).
- Reports from investors or hospitality groups of anomalous due diligence experiences (competitor foreknowledge, unexplained friction) consistent with information leakage.

## 16. Collection Priorities for Defenders

The structural exposure documented above establishes feasibility. The next analytical priority is to determine where that exposure translates into durable access, repeated abuse, or commercially relevant compromise.

### Priority Intelligence Requirements (PIRs)

- **PIR-1.** Empirical confirmation of surveillance asset concentration around tourism-facing and investor-relevant properties, consistent with the scenario assumptions in Section 9.
- **PIR-2.** Property-level confirmation that guest Wi-Fi networks and surveillance devices reside on the same subnet within representative commercial properties (riads, guesthouses, workshops). Section 8 documents the absence of enterprise-grade segmentation at corridor scale; per-property internal topology requires inspection access.
- **PIR-3.** Empirical evidence of reused business identifiers, phone numbers, or branding assets appearing across fake listings or impersonation workflows in patterns consistent with surveillance-enabled identity aggregation.
- **PIR-4.** Empirical evidence of access resale or fraud activity referencing hospitality, property rental, or local business infrastructure in Fez or comparable Moroccan heritage cities.

### What Would Increase Analytical Confidence

- Property-level confirmation of flat network segmentation across representative riad and guesthouse sample.
- Repeated enumeration of the same device clusters across multiple observation windows (confirming persistence, not just snapshot presence).
- Fraud cases showing verifiable overlap with locally observable identity fragments (business names, logos, phone numbers).
- Reporting or telemetry indicating resale of footholds tied to Moroccan hospitality infrastructure on access broker markets.

# 17. Implications and Recommendations

### Decision Implications

Risk here is primarily inherited rather than introduced. Entering a Medina-adjacent environment means taking on the network topology and surveillance exposure of the surrounding area. The usual enterprise mental model, with a perimeter, controlled access, and a known device inventory, does not map onto what is actually here.

- **Hospitality brands.** May inherit latent identity and reputational risk if properties are associated, via shared network topology or observable surveillance, with fraudulent listings using authentic local imagery and credentials.
- **Tech investors.** May encounter hybrid environments where standard security due diligence checklists (firewalls, application security, IT audits) fail to surface the structural risk created by flat consumer networks and shared ISP infrastructure.
- **Real estate and services.** Due diligence processes are not currently calibrated to assess informal digital infrastructure. A property with no detectable IT vulnerabilities in conventional terms may sit within a network environment where surveillance access, identity aggregation, and competitive intelligence collection are structurally feasible.

### Mitigation Recommendations

#### *For Micro-Business Operators (Riads, Guesthouses, Workshops)*

- **Network segmentation.** Implement separate VLANs or SSIDs for surveillance traffic, guest Wi-Fi, and management traffic. Most ISP-provided routers, including Arcadyan platforms, support basic VLAN or multiple-SSID configuration. The barrier is awareness, not hardware.
- **Disable WPS.** WPS PIN mode should be disabled on all access points. This eliminates the primary Layer 2 PIN-cracking attack vector at zero cost. WPS Push-Button (PBC) mode is lower risk but should also be disabled except during active pairing.
- **Firmware inventory and update cycle.** Establish a minimal inventory of devices reachable from the internet (cameras, NVR, routers) and apply vendor firmware updates. Priority: Hikvision and Dahua platforms, both of which have published patches for the CVEs cited in this assessment.
- **Disable UPnP and unnecessary port forwarding.** Many routers enable UPnP by default, allowing connected devices to open external ports automatically. Disabling UPnP removes a common mechanism by which surveillance devices become reachable from the public internet without the operator knowing.

#### *For Foreign Investors Conducting Due Diligence*

Red flags to assess during property or partnership evaluation:

- Shared ISP credentials across multiple properties.

- Absence of device inventory for any equipment exposed to the public internet.
- Flat network topology (guest Wi-Fi sharing subnet with surveillance or POS systems).
- Reliance on consumer-grade equipment for commercial operations.
- RTSP or HTTP admin interfaces accessible from public internet.

Include network architecture review and basic device inventory as standard components of operational due diligence in emerging market environments. These are market entry risk assessments, not IT audit functions.

***For Technology Vendors Targeting MENA Hospitality***

- Design for zero-trust architecture. Assume flat networks and shared credentials as default deployment conditions. Do not assume segmentation or per-user authentication exists.
- Prefer local processing over cloud relay to reduce the attack surface introduced by P2P cloud relay dependencies.
- Provide simplified segmentation tools, including wizard-based VLAN configuration or pre-configured dual-SSID setups accessible to non-technical operators. Security improvement requires usability investment, not just feature availability.

# 18. Generalisation and Strategic Outlook

### Generalisation and Transferability

The Medina of Fez illustrates a repeatable pattern: high-density urban environments where social trust governs access, consumer-grade ISP hardware is uniform, and legacy surveillance infrastructure operates without lifecycle management. Comparable conditions are observable in the Marrakech Medina, the Tunis Medina, Khan el-Khalili in Cairo, and historic cores of West African coastal cities. The model is not MENA-specific, but the documentation here is.

### Risk Trajectory (12 to 36 Months)

Risk is assessed as likely to increase over the 12 to 36 month horizon, driven by three compounding dynamics:

- **Digitalisation of micro-businesses.** Morocco's economic modernisation agenda (e-payment adoption, tourism platform integration, digital registration for informal businesses) is migrating commercial operations into digital infrastructure without commensurate security uplift. New digital attack surface is being created faster than security awareness is being built.
- **Persistence of legacy surveillance infrastructure.** The 2018 to 2020 firmware cohort, the most CVE-dense generation in the assessed dataset, is unlikely to be replaced within 12 to 36 months in the absence of a targeted remediation program. Device lifecycles in cost-constrained micro-business environments typically extend 5 to 10 years.
- **Increasing value of contextual identity.** As Morocco's investment profile rises (2030 World Cup infrastructure, CFC expansion, Tangier-Med supply chain growth), the commercial value of the identity fragments observable from within these environments increases proportionally. Access that was low-value in 2022 is higher-value in 2026 and will be higher still in 2029.

### Bottom Line

The Medina of Fez should be treated as a hybrid exposure environment in which remotely observable surveillance assets and trust-based local connectivity create access conditions that would be exploitable by financially motivated and intelligence-adjacent actors typical of comparable environments. Confidence is HIGH

on structural exposure, MODERATE on concentration estimates, and LOW on attribution absent victim-side telemetry. No claim of confirmed adversarial activity is made or implied.

## 19. About this Assessment

This assessment was produced independently by Rob Pinna, a cyber threat intelligence analyst with thirteen years of recurring field work in Morocco. The methodology integrates open-source intelligence, digital footprint analysis, and field research conducted directly in the environments assessed.

**Author.** Rob Pinna. CompTIA Security+, EC-Council Certified Threat Intelligence Analyst (CTIA). Published research at robpinna.com.

**Production context.** Independent analytical deliverable.

**Methodological transparency.** All data sources are passive and publicly accessible. The remote OSINT enumeration used Shodan and Censys with documented query patterns and covers the Fez metropolitan area. The field survey used WiGLE wardriving in public space along the three principal tourist arteries of Fes el-Bali (Tala'a Sghira, Tala'a Kebira, the Bab Rcif corridor), with all identifying data removed prior to analysis. The two layers of empirical evidence operate at different geographic scopes (Sections 5 and 6). No active exploitation, credential testing, or unauthorised network access was conducted.

**Analytical posture.** While the assessment is framed for investors and decision-makers, the long-term impact of unchecked exposure falls primarily on local residents. Effective security improvements benefit residents first, and commercial stakeholders by extension.

**Disclaimers.** This document does not constitute legal advice or regulatory guidance. It assesses exposure feasibility in structural terms. It does not confirm compromise of any specific entity, property, or system.

**Contact.** Constructive feedback and follow-up collaboration are welcome via robpinna.com.

# 20. Sources Consulted

The following public sources informed the methodology, technical references, and contextual framing of this assessment. Sources are grouped by category. Citations are provided in identifier form rather than full URL; identifiers are sufficient to locate the original material via standard web search or platform navigation.

### Technical Vulnerability References

CVE identifiers are drawn from the NIST National Vulnerability Database (NVD). Each entry can be retrieved by querying the CVE ID at nvd.nist.gov.

- NIST NVD: CVE-2017-7921 (Hikvision authentication bypass and hardcoded credentials).
- NIST NVD: CVE-2021-36260 (Hikvision unauthenticated command injection, CVSS 9.8 critical).
- NIST NVD: CVE-2021-33044 (Dahua authentication bypass, Magic Packet variant).
- NIST NVD: CVE-2021-33045 (Dahua authentication bypass, related variant).
- Viehboeck, S. (2011). Brute forcing Wi-Fi Protected Setup. Independent technical disclosure documenting the WPS PIN keyspace reduction flaw.
- Heffner, C. (2011). Cracking WiFi Protected Setup with Reaver. Independent concurrent disclosure of the same protocol weakness.

### Methodology and Analytical Standards

- Office of the Director of National Intelligence: Intelligence Community Directive 203 (ICD-203), Analytic Standards. Reference framework for estimative language and confidence calibration used throughout this assessment.
- MITRE ATT&CK Framework, version 15. Reference taxonomy for adversary technique mapping. Available at attack.mitre.org.
- MITRE Corporation: Common Vulnerabilities and Exposures (CVE) program. Identifier registry for publicly disclosed vulnerabilities.

### Open-Source Intelligence Platforms

- Shodan: internet-connected device search engine used for passive enumeration of RTSP, HTTP, and HTTPS endpoints attributed to Fez-area IP ranges.
- Censys: certificate transparency and host enumeration platform used as a secondary verification source for Shodan results.
- WiGLE (Wireless Geographic Logging Engine): community-contributed wireless network database used for the proximity survey methodology and OUI cross-reference.
- IEEE OUI Registry: hardware vendor identification reference for MAC address prefix attribution. Available at standards.ieee.org.
- Hurricane Electric BGP Toolkit: ASN and IP allocation reference used for ISP-level filtering (Maroc Telecom AS6713).

### Regulatory and Policy References

- Royaume du Maroc, Loi 09-08 (2009): Law on the protection of natural persons with regard to the processing of personal data. Primary Moroccan data protection legislation.
- Royaume du Maroc, Loi 05-20 (2020): Law on Cybersecurity. Establishes national cybersecurity framework and critical infrastructure obligations.

- CNDP (Commission Nationale de contrôle de la Protection des Données à caractère Personnel): public guidance and enforcement publications.
- DGSSI (Direction Générale de la Sécurité des Systèmes d'Information): public advisories and national cybersecurity guidance.
- maCERT: incident response coordination and threat advisory publications.

### Demographic and Urban Context

- Haut-Commissariat au Plan (HCP), Morocco: census-adjacent urban planning and demographic data used for Fez and Medina population estimates.
- UNESCO World Heritage Centre: documentation on the Medina of Fez as a designated World Heritage site, used for spatial and demographic context.
- Secondary OSINT on Moroccan tourism density, riad accommodation distribution, and Medina commercial structure, drawn from publicly available tourism industry reporting and academic urban studies literature.

### Comparative Environments

Cross-references to comparable heritage urban environments (Marrakech Medina, Tunis Medina, Khan el-Khalili, Dakar and Abidjan historic cores) are based on published academic and policy literature on informal digital infrastructure in MENA and West African urban contexts. These references support the generalisation argument in Section 18 but were not the subject of primary collection in this assessment.

### Note on Source Reliability

Technical references (NVD, MITRE, IEEE) are treated as authoritative within their domains. Regulatory references reflect publicly available legislation and guidance as of the collection window. Demographic figures should be read as reasonable estimates rather than precise counts, given the known difficulties of measuring informal urban populations.