IoT Device Vulnerability Assessment Overview Report

1. Executive Summary

This report provides an overview of the vulnerability assessment conducted on the selected IoT devices. The objective is to identify security weaknesses and provide actionable recommendations to improve the overall security posture.

2. Assessment Scope

Device Name	Model	IP Address	Firmware Version
Smart Sensor	SS-200	192.168.0.10	v1.0.5
Wireless Camera	WC-100	192.168.0.12	v2.2.0

3. Methodology

- Information Gathering
- Vulnerability Scanning
- Manual Verification
- Risk Assessment

- OWASP IoT Top 10
- CVE Database Cross-Reference
- Configuration Review

4. Key Findings

Vulnerability	Device	Risk Level	Status
Default Credentials	Smart Sensor	High	Unresolved
Outdated Firmware	Wireless Camera	Medium	Unresolved
Unsecured HTTP Communication	Both Devices	High	Unresolved

5. Recommendations

- Change all default credentials and enforce strong password policies.
- Update device firmware to the latest versions.
- Enable encrypted communication protocols (e.g., HTTPS, TLS).
- Implement regular vulnerability assessments and patch management.

6. Conclusion

Regular vulnerability assessments are vital to maintain IoT device security. Addressing the identified issues will reduce the risk of unauthorized access and data breaches.