# Home Network Security Assessment Report

# **Executive Summary**

A basic vulnerability assessment was conducted on the home network consisting of personal devices, a router, smart IoT devices, and a guest Wi-Fi segment. The goal was to identify misconfigurations, security gaps, and recommend mitigations based on best practices.

# **Network Environment Summary**

Device/Segment	IP Address	Role
Home Router	192.168.0.1	Gateway/DHCP
Work Laptop	192.168.0.101	Primary Device
Smart TV	192.168.0.110	IoT Device
Guest Wi-Fi	192.168.1.0/24	Guest Network
Network Printer	192.168.0.120	Peripheral

# **Findings Summary**

ID	Title	Severity	CVSS	Status
001	Default Router Login Enabled	High	8.8	Open
002	No Guest Wi- Fi Isolation	Medium	6.0	Open
003	Outdated Firmware – Router	High	7.5	Open
004	UPnP Enabled	Medium	5.3	Open
005	Weak Wi-Fi Encryption (WPA)	High	9.0	Open

006	Open Port 9100 on Printer	Low	4.0	Accepted
007	No DNS over HTTPS (DoH)	Informational	N/A	Open

# **Detailed Findings**

### 001 - Default Router Login Enabled

Severity: High

Affected System: 192.168.0.1

Description: The admin interface still uses default credentials (admin:admin). This

exposes the entire network to full compromise.

NIST Control: AC-2, AC-3

Recommendation: Change admin credentials immediately. Disable remote access to the

router interface.

#### 002 - No Guest Wi-Fi Isolation

Severity: Medium Affected System: N/A

Description: Devices connected to guest Wi-Fi can communicate with the internal LAN.

NIST Control: SC-7

Recommendation: Enable AP isolation on the guest Wi-Fi network.

#### 003 - Outdated Firmware - Router

Severity: High

Affected System: N/A

Description: Router firmware version is 2 years old and has known vulnerabilities (CVE-

2021-20090).

NIST Control: SI-2, CM-2

Recommendation: Upgrade firmware to the latest version after backing up configuration.

#### 004 - UPnP Enabled

Severity: Medium Affected System: N/A

Description: UPnP allows internal devices to open ports on the firewall automatically.

NIST Control: N/A

Recommendation: Disable UPnP in router settings unless absolutely required.

# 005 - Weak Wi-Fi Encryption (WPA)

Severity: High

Affected System: N/A

Description: Wi-Fi is using WPA (not WPA2/WPA3).

NIST Control: SC-12

Recommendation: Upgrade to WPA2 or WPA3. Use strong passphrases.

## 006 - Open Port 9100 on Printer

Severity: Low

Affected System: N/A

Description: Port 9100 used for raw printing is exposed and could be misused.

NIST Control: N/A

Recommendation: Disable if not needed. If needed, limit access to trusted IPs.

### 007 - No DNS over HTTPS (DoH)

Severity: Informational Affected System: N/A

Description: All DNS traffic is in plaintext.

NIST Control: N/A

Recommendation: Use DoH-capable resolvers like Cloudflare (1.1.1.1) or Google

(8.8.8.8).

#### **Tools Used**

Nmap – Port Scanning & Service Discovery

Router Interface Review

Shodan – External footprint checking

Firmware CVE Lookup – CVE Details

Wireshark – DNS analysis

Dradis-style format for documentation

# **Risk Score Summary**

Severity	Count
High	3
Medium	2
Low	1
Info	1

### **Recommendations**

- 1. Update all credentials for router, IoT, and admin interfaces.
- 2. Segment networks using VLAN or strict guest Wi-Fi isolation.
- 3. Patch firmware and software regularly for all devices.
- 4. Disable UPnP unless explicitly required.
- 5. Use WPA2/WPA3 with strong passwords.
- 6. Consider installing a Pi-hole or home firewall appliance for network DNS logging and ad blocking.

### **Conclusion**

This report reflects the current risk landscape of a home network. By applying the recommendations above, overall network security posture can be significantly improved.