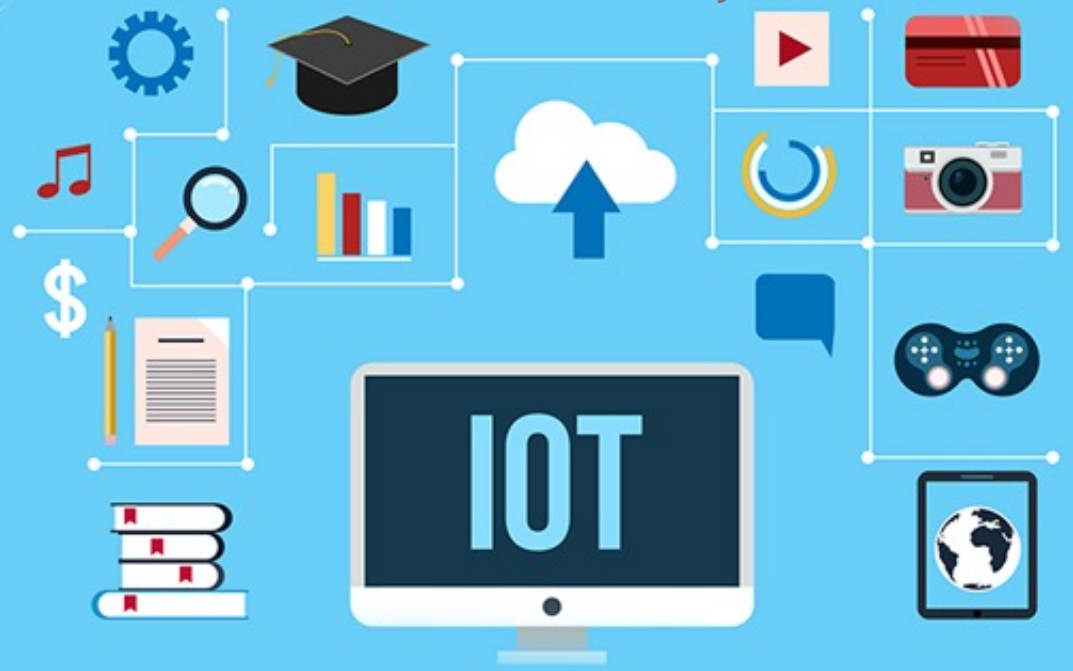
School of Computer Science and Engineering

Sacred Heart University



Vulnerability Assessment for IoT-Based Smart Homes

By: Bandar Almutairi

Agenda

- Project Problem Statement
- Goals and Objectives
- Scope
- Research Process
- Project Timeline
- Adopted Vulnerability Assessment Methodology for IoT devices
- Lab Environment
- Vulnerabilities Assessment Results & Recommendations
- Risk Score level

Project Problem Statement

- The proposed research will be about identifying the vulnerabilities in IoT devices and give the user an overview of the risks associated with IoT.

Goals and Objectives

Security Vulnerabilities Of IoT

Recommendation

scope

5 IoT
DEVICES

VULNERABILITY
ASSESSMENT

VULNERABILITY
VALIDATION

IMPACT ANALYSIS

Recommendation

Research Process

5 IoT
DEVICES

Nessus™

WIRESHARK

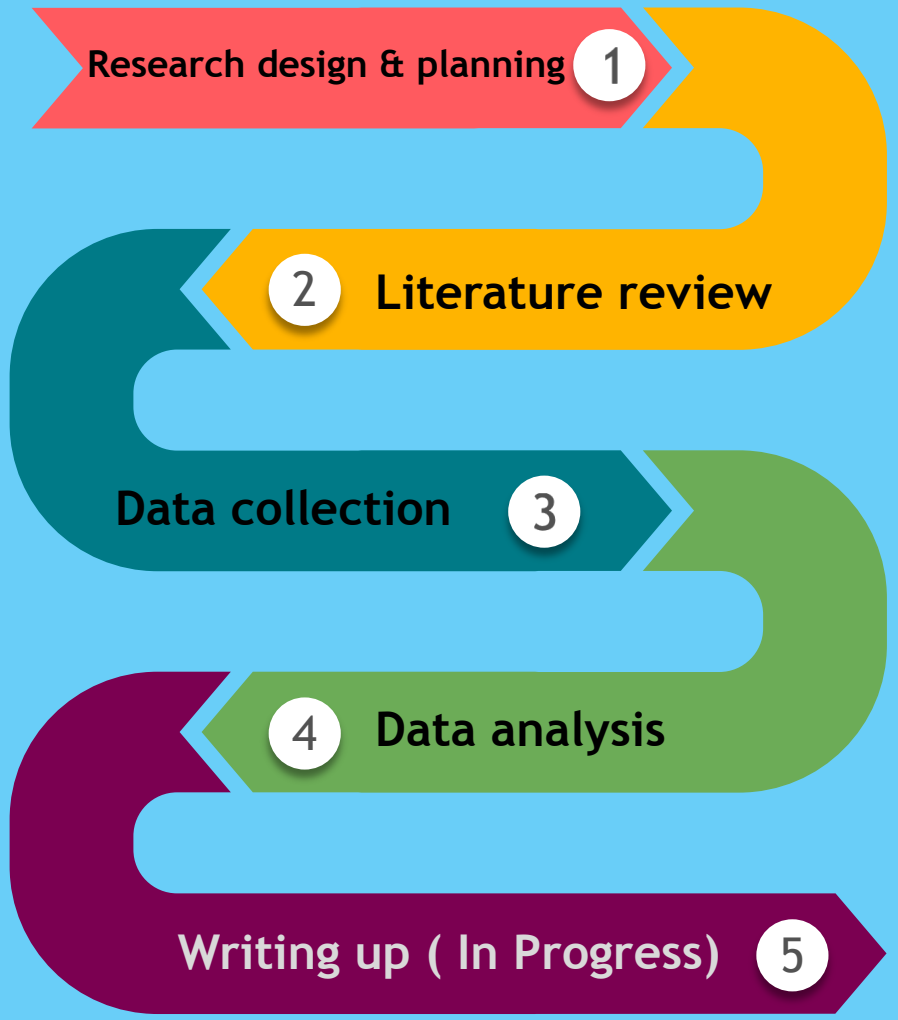
NMAP PROJECT

VULNERABILITY
ASSESSMENT

Recommendations

Project Timeline

Start: 09 September 2018



End: 29 November 2018

Adopted Vulnerability Assessment Methodology for IoT devices

1 RECONNAISSANCE

2 SCANNING

3 VULNERABILITY ASSESSMENT

ENVIRONMENT

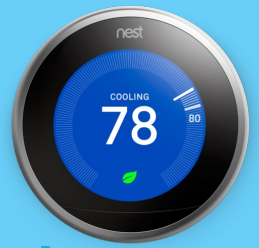
EPSON PRINTERS WORKFORCE 3620

SMART PLUG WI-FI MINI OUTLET ANEKEN

SAMSUNG SMART TV

Local Area Network

TEST MACHINE



nest THERMOSTAT

amazon fireTV

VALNERABILITIES ASSESSMENT

Epson printers workforce 3620

SPECIFICATIONS

OPEN PORTS

HOT DETAILS

VULNERABILITIES

RECOMMENDATIONS

PRINTERS

Product Code
C11CD19201

Model Number
C481D

Vendor
Epson

Model Name
WF-3620

Serial Number
SEDY14707

Device Management Protocol
SSL/TLS

Product Name
WorkForce WF-3620

Connectivity
Ethernet

OPEN PORTS

Port	Protocol	State	Service
80	TCP	Open	upnp
139	TCP	Open	netbios-ssn
433	TCP	Open	hhtp
445	TCP	Open	Microsoft-ds
515	UDP	Open	printer
613	UDP	Open	upnp
9100	UDP	Open	jetdirect
137	UDP	Open	netbios-ns
138	UDP	Open-Filtered	netbios-dgm
161	UDP	Open	snmp
427	UDP	Open-Filtered	svrloc
513	UDP	Open-Filtered	who
1022	UDP	Open-Filtered	exp2
1023	UDP	Open-Filtered	unknown
1067	UDP	Open-Filtered	instl_boots
3702	UDP	Open-Filtered	ws-discovery
5353	UDP	Open-Filtered	mdns
5355	UDP	Open-Filtered	llmnr
9200	UDP	Open-Filtered	wap-wsp
21525	UDP	Open-Filtered	unknown
28973	UDP	Open-Filtered	unknown
41446	UDP	Open-Filtered	unknown

Epson printers workforce 3620

HOT DETAILS

Type	Details
Operating System	Linux 2.6.31 - 2.6.35 (Embedded)
Open Ports	22
Filtered Ports	12
Scanned Ports	2000
IPv4	192.168.0.7
MAC	AC:18:26:46:94:EE

Risk Score level

Nessus™

Critical High Medium Low

Qualys®
Continuous Security

Degree of each category from 1 to 5

Minimal (1) Medium (2) Serious (3) Critical (4) Urgent (5)

Vulnerabilities

Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP)

High Medium Low

EPSON PRINTERS WORKFORCE 3620

VULNERABILITIES

01 — SNMP V1/ v2 Protocol Detected

5

An unsecure protocol which cannot ensure the confidentiality, integrity, and Authentication of data exchanged between printer and users.

02 — SNMP Agent Default Community Name (public)

This information can be guessed by attacker to gain more knowledge about the printer.

03 — Readable SNMP Information

3

give unauthorized users an incredible amount of valuable and sensitive information about your network.

RECOMMENDATION

01 Disable or remove SNMP v1/v2 authentication and Use SNMP version 3 authentication which provides additional security features.

02 Change the default community string.

03 Replace the default password (often "public" or "private") with a secure one. The password should be hard to guess.

Nessus™ — Critical | High | Medium | Low

Qualys — Degree of each category from 1 to 5: 1- Minimal 2- Medium 3- Serious 4- Critical 5- Urgent — Vulnerabilities | Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP) — High | Medium | Low

EPSON PRINTERS WORKFORCE 3620

VULNERABILITIES

04 SSL V2 & V3 Protocol Detection

SSL Version 2 & 3 is affected by several cryptographic flaws. This is can be a result of a MITM attach or decrypt the communications between the affected printer and users.

05 SSL v3 Padding Oracle Attack Information Disclosure

The attacker tricks the browser into connecting with SSLv3 and gain access to encrypted communication.

06 SSL Self-Signed Certificate

The certificate is not signed by a known certificate authority. This can establish a MITM attack against the printer.

RECOMMENDATION

04 Use TLS 1.1 with recommended cipher suites only for ensuring communication security.

05 Disable SSL 2.0 and 3.0. by Consult the application's documentation to avoid this vulnerability

06 Purchase or generate a proper certificate for this service.

Nessus Critical High Medium Low

Qualys. Degree of each category from 1 to 5
1- Minimal 2- Medium 3- Serious
4- Critical 5- Urgent
Vulnerabilities Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP) High Medium Low

EPSON PRINTERS WORKFORCE 3620

VULNERABILITIES

HTTP Security Headers

2 07

Headers were not configured on the management interface of the printer.

Application Error Disclosure

08

The login interface of the printer shows an error/warning message that may disclose sensitive information.

SMB Signing Disabled / Not Required

3 09

SMB signing is disabled on both the client and server. Sessions are unauthenticated which can allow MITM attacks against the SMB server.

RECOMMENDATION

Enable HTTP security headers on all web pages of printer web interface — 07

Implement password checker at the stage of user accounts creation. Allow complex passwords only. — 08

Enabled SMB sign. — 09

Nessus™ Critical High Medium Low

Qualys. Degree of each category from 1 to 5
1- Minimal 2- Medium 3- Serious
4- Critical 5- Urgent
Vulnerabilities Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP) High Medium Low

VALNERABILITIES ASSESSMENT

Smart Plug Wi-Fi Mini Outlet Aneken

SPECIFICATIONS

OPEN PORTS

HOT DETAILS

VULNERABILITIES

RECOMMENDATIONS

Smart Plug

Model Number
SW A1

Product Type
Smart Plug

Wireless IEEE standards
WIFI 2.4 GHz b/g/n

Device Name
Smart WIFI Socket

Security Mechanism
WEP/WPA-PSK/WPA2-PSK

Security Type
WEP64/WEP128/TKIP/CCMP

OPEN PORTS

Port	Protocol	State	Service
6668	TCP	Open	irc
49145	UDP	Open	unknown

Smart Plug Wi-Fi Mini Outlet Aneken

HOT DETAILS

Type	Details
Operating System	OSRAM Lightify ZigBee gateway
Open Ports	2
Filtered Ports	1
Scanned Ports	2000
IPv4	192.168.0.12
MAC	68:C6:3A:99:31:12

SMART PLUG WI-FI MINI OUTLET ANEKEN

VULNERABILITIES

01

Non-Zero Padding Bytes Observed in Ethernet Packets

packets from the host were padded to the minimum size using non-zero padding bytes which may be exploited to fingerprint the Ethernet cards and device drivers.

RECOMMENDATION

01

Contact the vendor of the Ethernet cards and device drivers for the availability of a patch.

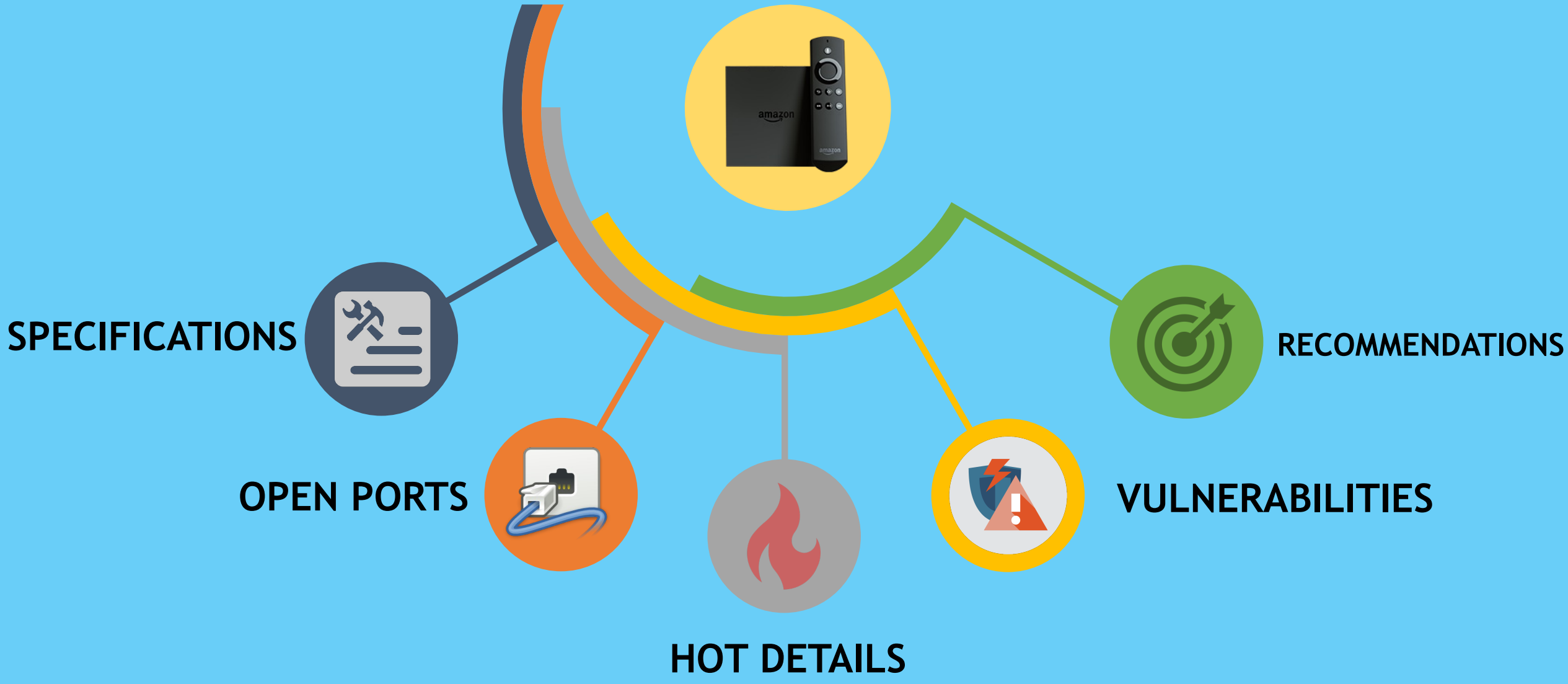
Nessus Critical High Medium Low

Qualys. Degree of each category from 1 to 5
1- Minimal 2- Medium 3- Serious
4- Critical 5- Urgent
Vulnerabilities Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP) High Medium Low

VALNERABILITIES ASSESSMENT

Amazon Fire TV



STREAMING DEVICE

Connectivity
Wifi 802.11 a/b/g/n/ac; 2x2 MIMO

Model Number
DV83YM

Vendor
Amazon

Model Name
Fire TV 2nd Generation

Serial Number
G070GV01536303E6

Software Version
6.0.9.1-014

Operation System
Fire OS 5 – Based on Android 5.1

Connectivity
Ethernet 10/100Mbs

OPEN PORTS

Port	Protocol	State	Service
5555	TCP	Open	freeclv
8008	TCP	Open	http
67	UDP	Open-Filtered	dhcps
199	UDP	Open-Filtered	smux
389	UDP	Open-Filtered	Ldap
999	UDP	Open-Filtered	Applix
1048	UDP	Open-Filtered	Neod2
1900	UDP	Open-Filtered	Upnp
2148	UDP	Open-Filtered	Veritas-ucl
5353	UDP	Open-Filtered	Zeroconf
19332	UDP	Open-Filtered	unknown
21525	UDP	Open-Filtered	unknown
30718	UDP	Open-Filtered	unknown
33249	UDP	Open-Filtered	unknown
46836	UDP	Open-Filtered	unknown
49152	UDP	Open-Filtered	unknown
49185	UDP	Open-Filtered	unknown
58178	UDP	Open-Filtered	unknown
64727	UDP	Open-Filtered	unknown

amazon fireTV

HOT DETAILS

Type	Details
Operating System	Amazon Kindle Paperwhite
Open Ports	21
Filtered Ports	19
Scanned Ports	2000
IPv4	192.168.0.6
MAC	F0:27:2D:B2:A1:FD

amazon fireTV

VULNERABILITIES

HTTP Security Headers

2 01

Headers were not configured on the management interface of the Fire TV. The headers that were not configured include X-frame-options header, X_XSS protection header and X-content-type- options header.

RECOMMENDATION

Enable all HTTP security headers on the Fire TV 01

Nessus™ Critical High Medium Low

Qualys. Degree of each category from 1 to 5
1- Minimal 2- Medium 3- Serious
4- Critical 5- Urgent
Vulnerabilities Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP) High Medium Low

VALNERABILITIES ASSESSMENT

Samsung Smart TV

SPECIFICATIONS

OPEN PORTS

HOT DETAILS

VULNERABILITIES

RECOMMENDATIONS

Smart TV

Connectivity
802.11ac Wi-Fi Built In

Vendor
Samsung

Model Number
UN55JU670D

Serial Number
03PQ3CCG700326P

Software Version
T-HKMAKUC-1530.1, BT-S

OPEN PORTS

Port	Protocol	State	Service
7676	TCP	Open	upnp
8000	TCP	Open	http-alt
8001	TCP	Open	http
8002	TCP	Open	http
8080	TCP	Open	http
9999	TCP	Open	abyss

Samsung Smart TV

HOT DETAILS

Type	Details
Operating System	Linux 3.2 -3.10
Open Ports	6
Filtered Ports	0
Scanned Ports	1000
IPv4	192.168.0.9
MAC	F8:04:2E:82:BA:42

SAMSUNG SMART TV

VULNERABILITIES

01 Multiple Stack-based Buffer Overflows RCE

The Portable SDK for UPnP TV (libupnp) library contains multiple buffer overflow vulnerabilities

02 SSL Self-Signed Certificate

The certificate is not signed by a known certificate authority. This can establish a man-in-the-middle attack against the Smart TV.

03 SSL Certificate Cannot Be Trusted:

Self-signed certificate or certificate is not valid at the time of the scan or it may contain a signature didn't match the certificate's information or could not be verified.

RECOMMENDATION

01 Apply an update to libupnp version 1.6.18 or later.

02 Purchase or generate a proper certificate for this service.

03 Purchase or generate a proper certificate for this service.

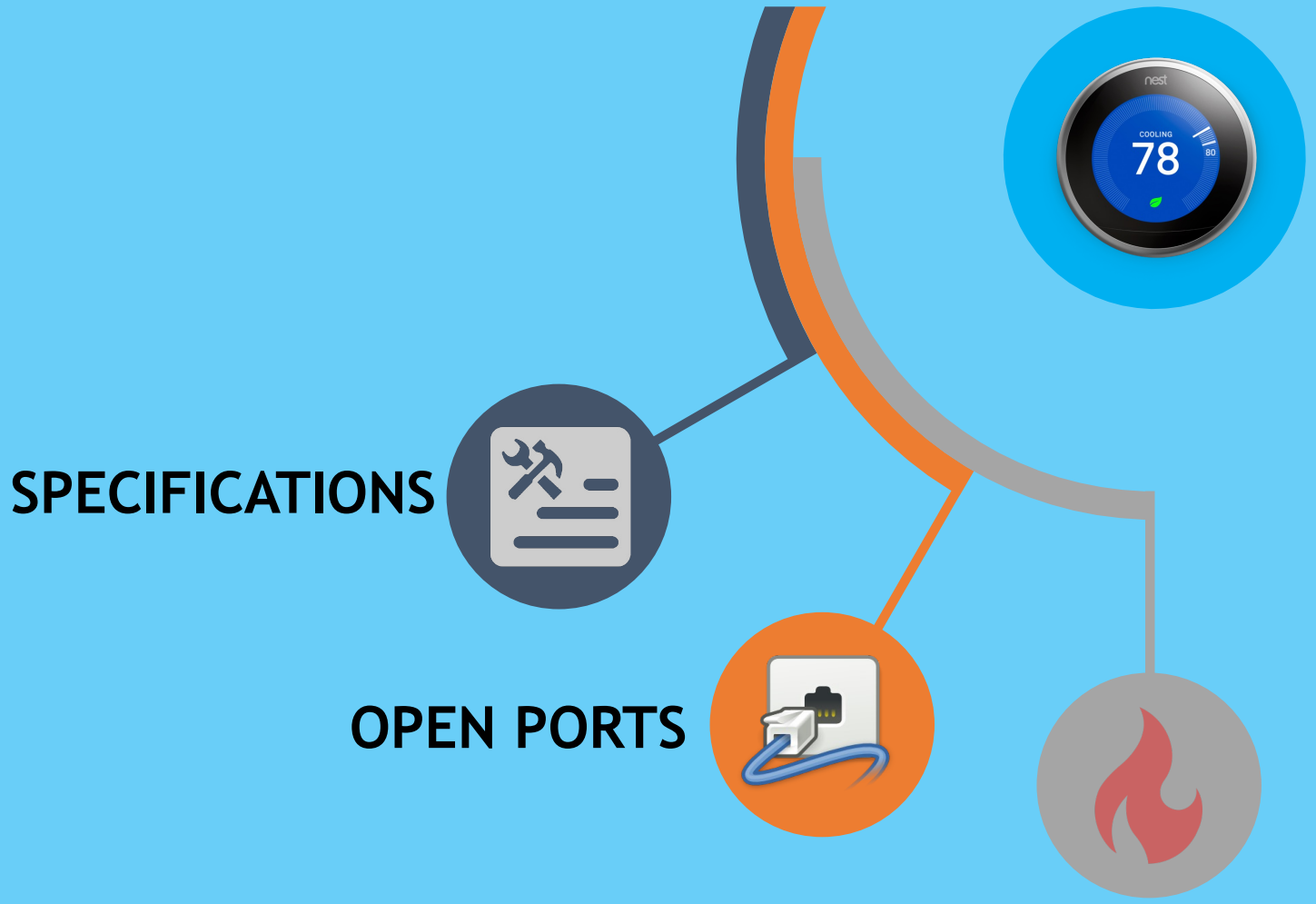
Nessus™ Critical High Medium Low

Qualys. Degree of each category from 1 to 5
1- Minimal 2- Medium 3- Serious
4- Critical 5- Urgent
Vulnerabilities Potential Vulnerabilities

OWASP Zed Attack Proxy (ZAP) High Medium Low

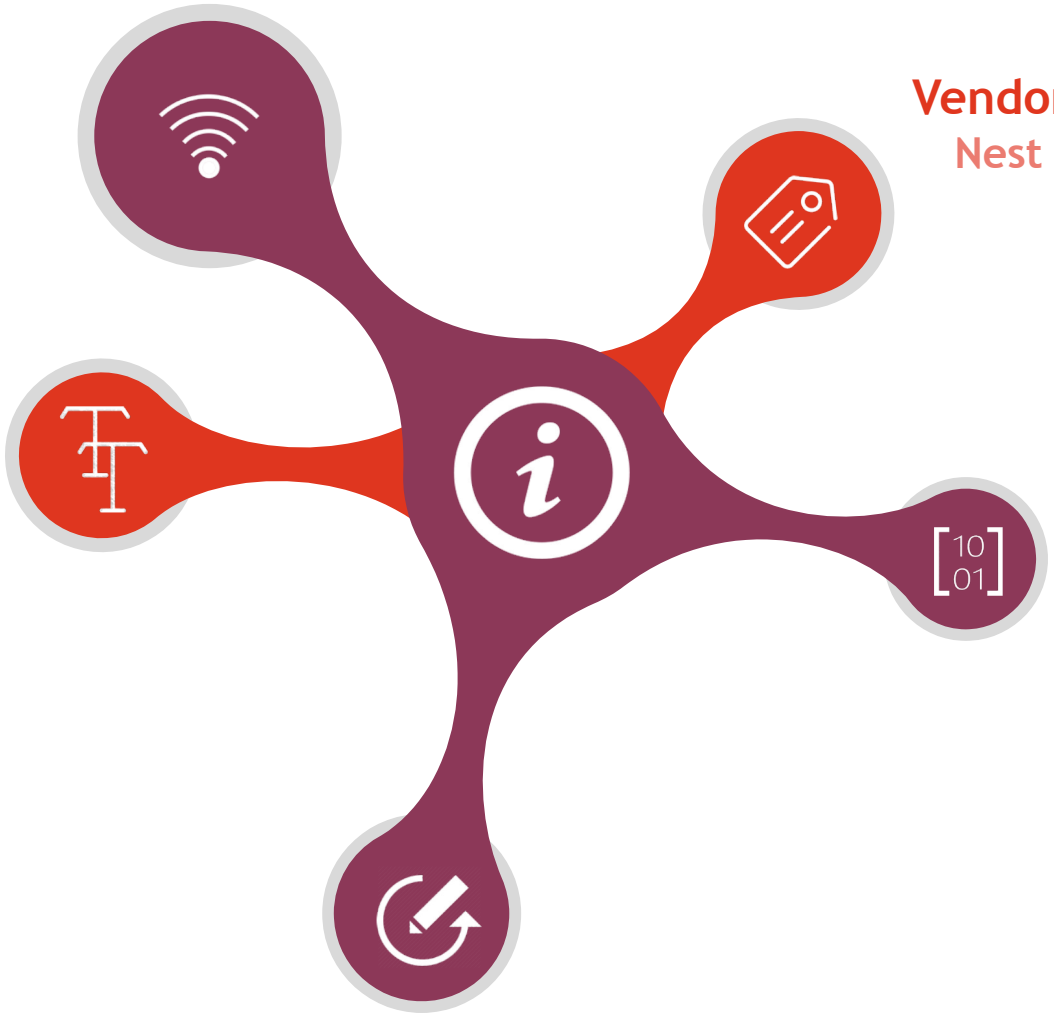
VALNERABILITIES ASSESSMENT

Nest smart thermostat



SMART THERMOSTA

Connectivity
Wi-Fi: 802.11b/g/n 2.4GHz



Vendor
Nest

Model Name
Display-3.4

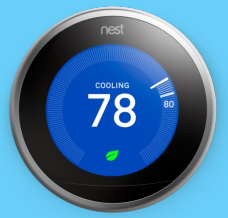
Serial Number
09AA01AC161708G1

Software Version
5.8.2-1

OPEN PORTS

Port	Protocol	State	Service

No Open ports found



nest THERMOSTAT

HOT DETAILS

Type	Details
Operating System	Linux 2.6.37
Open Ports	0
Filtered Ports	0
Scanned Ports	2000
IPv4	192.168.0.11
MAC	18:B4:30:C2:59:76