Commercial In Confidence

ProCheckUp

CYBER SECURITY EXPERTS

Technical Report
IoT Device Testing Based on the IoT Security Compliance framework (Release 1.1)
Level 1 devices
onlyXX/XX/20XX

Customer

DATE

Contents

Non-Disclosure Statement & Legal Notice

Non-Disclosure Statement

This report has been made for Customer. All information obtained during a ProCheckUp assessment about our customer's systems and assets including, but not limited to, its procedures and systems, is deemed privileged information and not for public dissemination. ProCheckUp Ltd pledge their commitment that this information will remain strictly confidential. This information will not be disclosed or discussed to any third party without the written consent of customer. ProCheckUp Ltd is fully committed to maintaining the highest level of ethical standards in its business practice.

Legal Notice

It is impossible to test a target environment for 100% security within normal timeframes. This report does not constitute and should not be construed as a guarantee of the target's security.

How to use this report

Executive Summary

This section provides an overview of the test background and details and gives an indication to the security posture of the overall environment.

Scope of Testing

This section details the scope agreed with Customer before ProCheckUp testing was conducted.

Restrictions on Testing

This section details any problems that occurred which disrupted or prevented testing.

Summary of Findings

This section gives a high-level summary of the main findings.

Test Results

This section details the results obtained whilst testing the targets and presents the HIGH to LOW severity vulnerabilities discovered. Each vulnerability includes an indication of its level of impact, a description, results and evidence and guidance on how it can be resolved. Finally, a list of associated references will be provided (where available) to enable the recipient to gain further understanding of the issue being presented.

CVSS Scoring System

ProCheckUp currently uses version 2 of the Common Vulnerability Scoring System (CVSS) when rating vulnerabilities discovered during security testing. CVSS is an open industry framework used to assess the severity of security vulnerabilities based on three distinct metrics:

- Base Metrics are associated with intrinsic characteristics of a vulnerability
- Temporal Metrics are associated with evolving characteristics of a vulnerability
- Environmental Metrics are associated with vulnerabilities that are dependent on environmental factors.

The outcome of these metrics is a score indicating the severity of the vulnerability and provides an accurate input to an enterprise prioritised approach to remediation. The CVSS scheme scores are grouped as follows:

- CVSS scored 10.0 would be considered CRITICAL severity
- CVSS scored 7.0-9.9 would be considered HIGH severity
- CVSS scored 4.0-6.9 would be considered Medium severity
- CVSS scored 0-3.9 would be considered as LOW severity

ProCheckUp use base metrics to build a traffic light system in their vulnerability reporting tables in the “Test Results” section of this report.

More information on the system we use to rate vulnerabilities can be found in Appendix A.
The CUSTOMER provided risk ratings guidelines used in this report can be found in Appendix B. As such the risk ratings calculated are on based on CUSTOMER provided guidelines and should not be taken as accurate.

Project Details

Item	Details
Testing Company	ProCheckUp Ltd
Website	www.procheckup.com
Project ID	IoT Device Testing
Test Location	ProCheckUp Ltd 4TH Floor Fairgate House 78 New Oxford Street London WC1A 1HB
Customer Contact	John Doe
Telephone	+44 (0) 161 XXX XXXX
Email	john.doe@customer.com
Consultant	Richard Roe
Consultant Details	Richard.roe@procheckup.com
Project Start	08/10/2018
Project Complete	13/10/2018

Document Control

Date	Action	Version	Author
19/10/2018	Initial Draft	0.1	John Doe
19/10/2018	General QA	0.2	Richard Roe
19/10/2018	Tech QA	0.4	John Doe
19/10/2018	Final Report	1.0	Richard Roe

1 Executive Summary

1.1 Introduction

On 8th October 2018, ProCheckUp was commissioned to perform an IOT (Internet Of Things) penetration test on a XXX and its hosting server. The solution provides remote power line monitoring for customers.

The XXX device under test had unnecessary USB ports externally exposed which recognised devices plugged in for instance a USB keyboard, the casing had no protective seals to determine if an intrusion had occurred.

Several issues were identified with the application's cloud API server. ProCheckUp identified some weaknesses in the encryption (TLS ciphers and versions), as well as too many ports exposed when connected to a Wi-Fi router. For instance, the mobile client uses port 8201 to communicate with XXX..

The Non-volatile flash drive was not encrypted or cryptographically paired to the processor, this allowed firmware files to be modified and the boot configuration files to be changed.

It is recommended the issues identified be resolved in a timely manner using the recommendations outlined within this report, with priority given to the medium rated issues.

1.2 Issues Identified

1.2.1 External analysis

This section identifies the issues discovered during the hardware analysis stage of this engagement. A summary of the most serious issues can be found in Section 4 (Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5 (Test Results).

Issue ID	Issue	Issue Rating
EXT-1	Too many network ports were found open:	MEDIUM
EXT-2	Outdated TSL1.0 protocol was found to be in use	MEDIUM
EXT-3	The product did not prevent unauthorized connections to it or other devices the product is connected to.	LOW
EXT-4	It was possible to gain access to the internal assembly without breaking seals.	LOW

1.2.2 Gaining shell access

This section identifies the issues discovered during the gaining shell access stage of this engagement. A summary of the most serious issues can be found in Section 4 (Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5 (Test Results).

Issue ID	Issue	Issue Rating
SH-1	Non-volatile flash device is not encrypted	MEDIUM
SH-2	Non-volatile flash device is not cryptographically paired to the processor	MEDIUM

1.2.3 Firmware analysis

This section identifies the issues discovered during the firmware analysis stage of this engagement. A summary of the most serious issues can be found in Section 4 (Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5 (Test Results).

Issue ID	Issue	Issue Rating
FW-1	Unauthenticated software and files could be loaded	MEDIUM
FW-2	The system did not have an irrevocable Secure Boot process.	MEDIUM
FW-3	The secure boot process was not enabled by default.	

		LOW

1.3 Recommended Actions

ProCheckUp recommend that the MEDIUM rated issues identified during this engagement should be subject to remedial work to ensure an increase in the security posture of the environment, to protect it from attack. The following prioritised approach is recommended:

1.3.1 Immediate Actions

- Only open necessary network ports
- Only support strong TLS ciphers and versions.
- Encrypt the non-volatile flash drive.

1.3.2 Medium Term Actions

- Cryptographically pair the non-volatile flash drive to the processor
- Adopt measures to prevent unauthenticated software and files being loaded
- Enforce an irrevocable secure boot process.

1.3.3 'Long Term Actions

- Restrict unauthorised connections to the device
- Use security seals on the case, to indicate if the device has been tampered with.

2 Scope of Testing

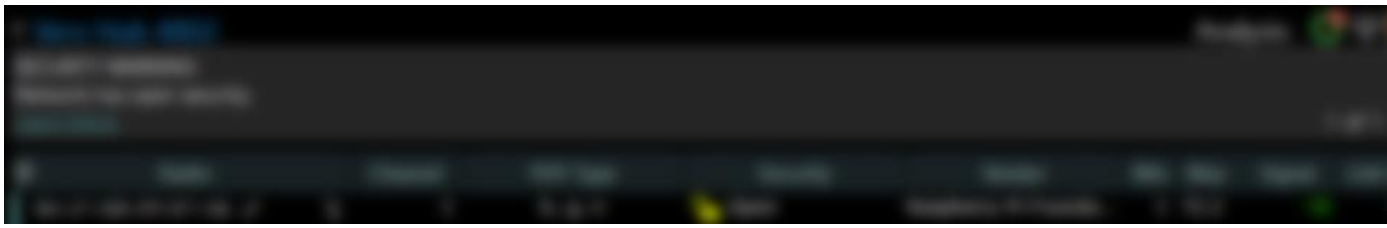
The scope for this engagement was agreed following e-mail communications between John Doe of Customer and John Smith of ProCheckUp. The scope was to perform a time limited 4 days IOT (Internet Of Things) test against an XXX device.

3 Restrictions on Testing

This was a time limited test, with only 4 days allocated for both infrastructure, application and IoT testing.

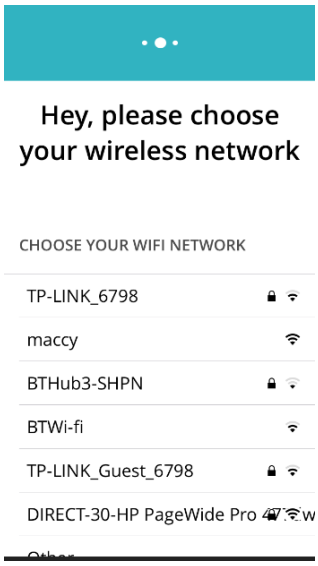
4 Hardware Overview

Initially the XXX hub acts as an open access point, and broadcasts itself awaiting connections.



Initially the software wants a XXX hub to be selected:

After connecting to the XXX hub, the Wi-Fi router is chosen:



LAN Turtle testing:

It was determined the USB ports did not function after boot, as normally attaching a LAN turtle to a Raspberry PI USB connector. Would allow the Lan Turtle to access the Raspberry PI's network interface.

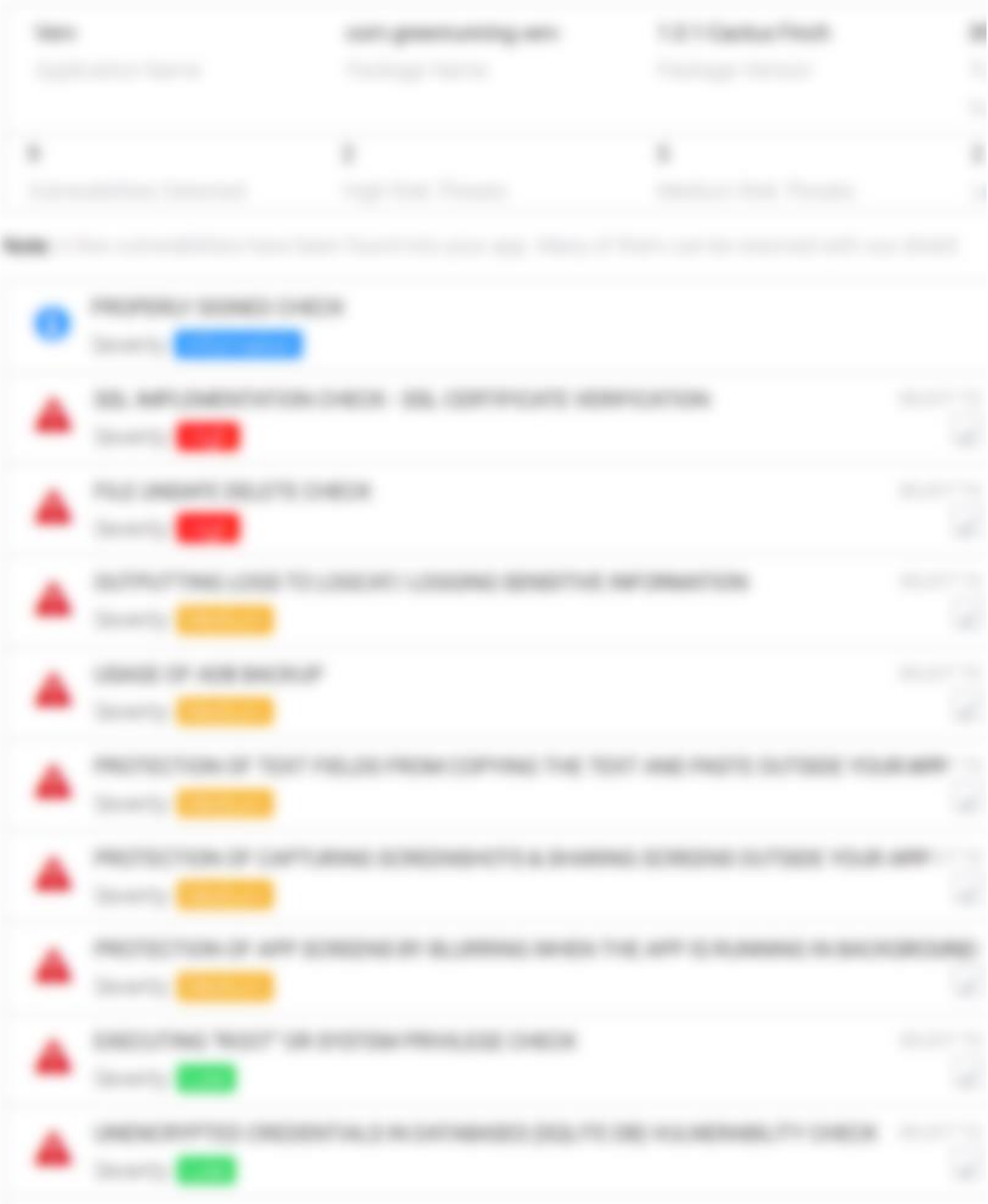
```
root@turtle:~# nmap -sP 172.:       -254

Starting Nmap 6.47 ( http://nmap.org ) at 2018-07-27 12:11 UTC
Nmap scan report for turtle.lan (172.16.84.1)
Host is up.
Nmap done: 254 IP addresses (1 host up) scanned in 10.61 seconds
root@turtle:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:13:37:A5:A1:56
          inet addr:172.         Bcast:172.           Mask:255.255.255.0
          inet6 addr: fe80::213:37ff:fea5:a156/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1020 errors:0 dropped:0 overruns:0 carrier:0
```

4.1 Analysis of the protocol used between the mobile client and API server

sslscan app-xxx.com (out of scope) – outdated protocol and medium strength ciphers used:

```
  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Preferred TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Preferred TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
```

Static analysis of the Android mobile client (out of scope) shows multiple vulnerabilities.



5 Test Results

1) Mapping the attack surface

This step helps the architecture of the solution to be understood and helps establish the various tests that would be run on the product, sorted by priority.

The architecture can broadly be divided into three categories:

1) Embedded device
   These devices include hubs, smart lightbulbs, motion sensors, smart switches and additional connected devices.

2) Firmware, software and applications
   After hardware testing the next component to be tested is software.
   This includes firmware running on the device, mobile applications which are used to manage the device and the cloud components connected to the device.

3) Radio communications
   Radio communications provide a way for some devices to communicate with each other. Some of the radio communications used are Cellular, Wi-Fi, Bluetooth low energy, Zigbee, Z-Wave and more.

2) Embedded device – hardware analysis

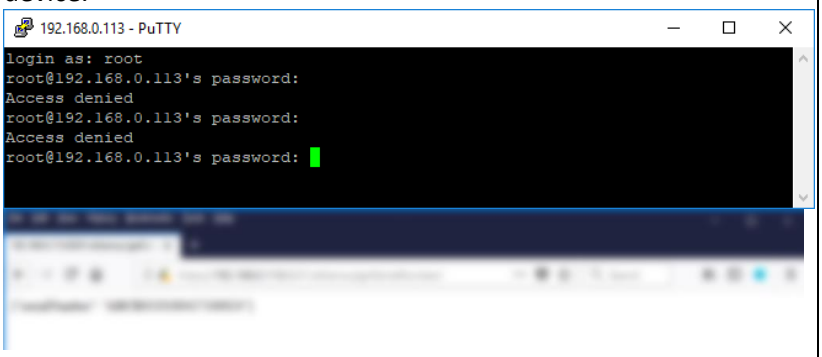
This stage allows us to understand the devices hardware from a security perspective by using both internal and external analysis. This consists of two stages:

1) External analysis
2) Internal analysis

External physical analysis

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
	FAIL: It was possible to gain access to the internal assembly without breaking seals: 			

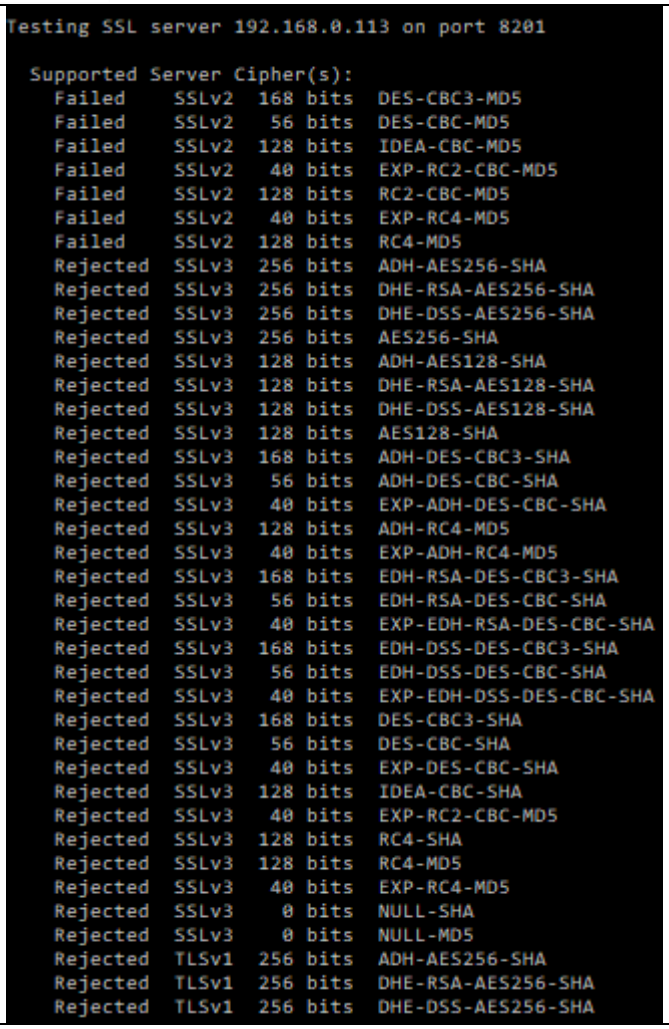
External network, USB and wireless interfaces tests, Cellular, Wi-Fi, Bluetooth low energy, Zigbee, Z-Wave and more.
Hardware tools: HackRF, LimeSDR, KillerBee, Open Sniffer, Ubertooth, BLE Sniffer, WIFI Pineapple Tetra, Bash Bunny
Software tools: BURPSuite Pro, Nessus Pro or SSLscan, Nmap. Wireshark

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.7.1	The product prevents unauthorised connections to it or other devices the product is connected to. For example, there is a firewall on each interface and internet layer protocol.	1 and above	M	TBD in future release
	FAIL: It was possible to connect to the device using both SSH and HTTPS from a laptop connected to the same Wi-Fi router as the XXX device.  			
2.4.7.2	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behaviour.	1 and above	M	TBD in future release

	FAIL:
	Too many ports were found open:
	`Starting Nmap 6.40 ( http://nmap.org ) at 2018-07-13 00:56 GMT Daylight Time`
	`mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.`
	` Try using --system-dns or specify valid servers with --dns-servers`
	`Nmap scan report for 192.168.0.113`
	`Host is up (0.022s latency).`
	`Not shown: 65525 closed ports`
	`PORT  STATE SERVICE`
	`22/tcp  open  ssh`
	`6223/tcp open  unknown`
	`6224/tcp open  unknown`
	`6225/tcp open  unknown`
	`6226/tcp open  unknown`
	`6323/tcp open  unknown`
	`6324/tcp open  unknown`
	`6325/tcp open  unknown`
	`6326/tcp open  unknown`
	`8101/tcp open  unknown`
	`8201/tcp open  trivnet2`
	`MAC Address: B8:27:EB:35:A0:B5 (Raspberry Pi Foundation)`
	`Starting Nmap 6.40 ( http://nmap.org ) at 2018-07-13 03:50 GMT Daylight Time`
	`Nmap scan report for 192.168.0.113`
	`Host is up (0.0037s latency).`
	`Not shown: 994 closed ports`
	`PORT  STATE  SERVICE`
	`123/udp  open  ntp`
	`3702/udp  open|filtered ws-discovery`
	`5353/udp  open  zeroconf`
	`10000/udp open|filtered ndmp`
	`19489/udp open|filtered unknown`
	`25546/udp open|filtered unknown`
	`MAC Address: B8:27:EB:35:A0:B5 (Raspberry Pi Foundation)`
	`Nmap done: 1 IP address (1 host up) scanned in 1164.87 seconds`			

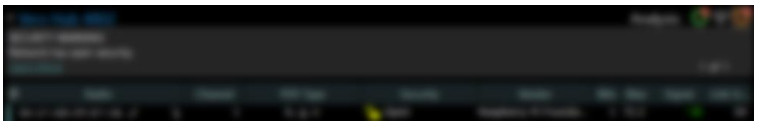
2.4.7.3	Products with one or more network interfaces, any uncontrolled, and unintended packet forwarding software should be blocked.	1 and above	M	TBD in future release
	PASS:			

	Connecting the Ethernet port disconnected the Wi-Fi port.			
2.4.7.4	Devices support only the latest versions of application layer protocols with no publicly known vulnerabilities and it should not be possible to downgrade a connection to an older, less secure version.	1 and above	M	TBD in future release
	PASS: No insecure SSL protocols were found to be used. Testing SSL server 192.168.0.113 on port 8101 Supported Server Cipher(s): Failed SSLv2 168 bits DES-CBC3-MD5 Failed SSLv2 56 bits DES-CBC-MD5 Failed SSLv2 128 bits IDEA-CBC-MD5 Failed SSLv2 40 bits EXP-RC2-CBC-MD5 Failed SSLv2 128 bits RC2-CBC-MD5 Failed SSLv2 40 bits EXP-RC4-MD5 Failed SSLv2 128 bits RC4-MD5 Rejected SSLv3 256 bits ADH-AES256-SHA Rejected SSLv3 256 bits DHE-RSA-AES256-SHA Rejected SSLv3 256 bits DHE-DSS-AES256-SHA Rejected SSLv3 256 bits AES256-SHA Rejected SSLv3 128 bits ADH-AES128-SHA Rejected SSLv3 128 bits DHE-RSA-AES128-SHA Rejected SSLv3 128 bits DHE-DSS-AES128-SHA Rejected SSLv3 128 bits AES128-SHA Rejected SSLv3 168 bits ADH-DES-CBC3-SHA Rejected SSLv3 56 bits ADH-DES-CBC-SHA Rejected SSLv3 40 bits EXP-ADH-DES-CBC-SHA Rejected SSLv3 128 bits ADH-RC4-MD5 Rejected SSLv3 40 bits EXP-ADH-RC4-MD5 Rejected SSLv3 168 bits EDH-RSA-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-RSA-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA Rejected SSLv3 168 bits EDH-DSS-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-DSS-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-DSS-DES-CBC-SHA Rejected SSLv3 168 bits DES-CBC3-SHA Rejected SSLv3 56 bits DES-CBC-SHA Rejected SSLv3 40 bits EXP-DES-CBC-SHA Rejected SSLv3 128 bits IDEA-CBC-SHA Rejected SSLv3 40 bits EXP-RC2-CBC-MD5 Rejected SSLv3 128 bits RC4-SHA Rejected SSLv3 128 bits RC4-MD5 Rejected SSLv3 40 bits EXP-RC4-MD5 Rejected SSLv3 0 bits NULL-SHA Rejected SSLv3 0 bits NULL-MD5 Rejected TLSv1 256 bits ADH-AES256-SHA Rejected TLSv1 256 bits DHE-RSA-AES256-SHA Rejected TLSv1 256 bits DHE-DSS-AES256-SHA Rejected TLSv1 256 bits AES256-SHA Rejected TLSv1 128 bits ADH-AES128-SHA Rejected TLSv1 128 bits DHE-RSA-AES128-SHA Rejected TLSv1 128 bits DHE-DSS-AES128-SHA Rejected TLSv1 128 bits AES128-SHA Rejected TLSv1 168 bits ADH-DES-CBC3-SHA Rejected TLSv1 56 bits ADH-DES-CBC-SHA Rejected TLSv1 40 bits EXP-ADH-DES-CBC-SHA			

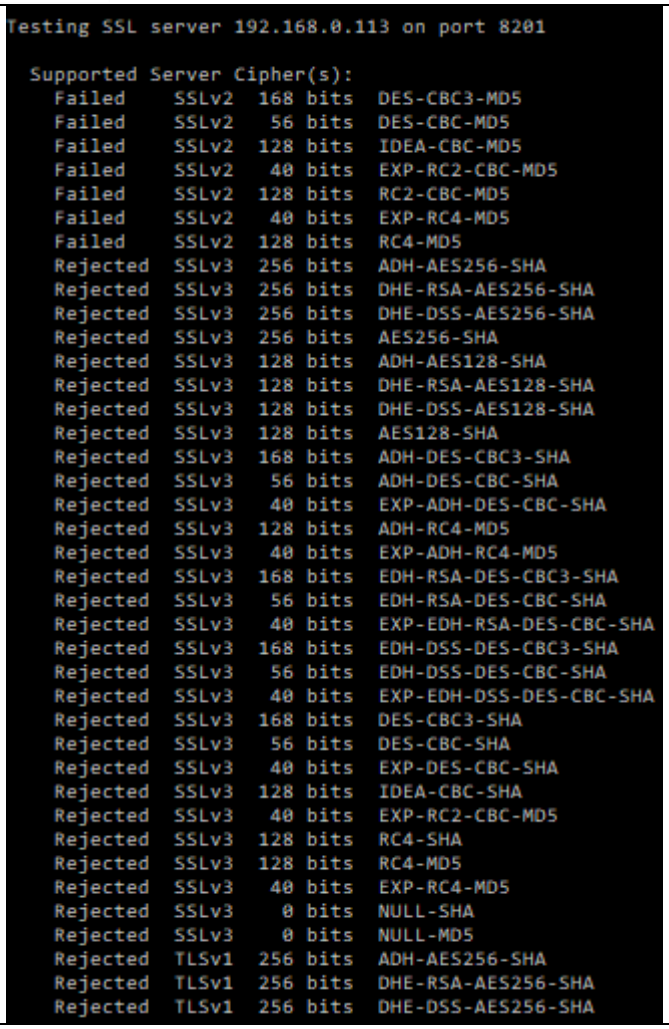
	 Testing SSL server 192.168.0.113 on port 8201 Supported Server Cipher(s): Failed SSLv2 168 bits DES-CBC3-MD5 Failed SSLv2 56 bits DES-CBC-MD5 Failed SSLv2 128 bits IDEA-CBC-MD5 Failed SSLv2 40 bits EXP-RC2-CBC-MD5 Failed SSLv2 128 bits RC2-CBC-MD5 Failed SSLv2 40 bits EXP-RC4-MD5 Failed SSLv2 128 bits RC4-MD5 Rejected SSLv3 256 bits ADH-AES256-SHA Rejected SSLv3 256 bits DHE-RSA-AES256-SHA Rejected SSLv3 256 bits DHE-DSS-AES256-SHA Rejected SSLv3 256 bits AES256-SHA Rejected SSLv3 128 bits ADH-AES128-SHA Rejected SSLv3 128 bits DHE-RSA-AES128-SHA Rejected SSLv3 128 bits DHE-DSS-AES128-SHA Rejected SSLv3 128 bits AES128-SHA Rejected SSLv3 168 bits ADH-DES-CBC3-SHA Rejected SSLv3 56 bits ADH-DES-CBC-SHA Rejected SSLv3 40 bits EXP-ADH-DES-CBC-SHA Rejected SSLv3 128 bits ADH-RC4-MD5 Rejected SSLv3 40 bits EXP-ADH-RC4-MD5 Rejected SSLv3 168 bits EDH-RSA-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-RSA-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA Rejected SSLv3 168 bits EDH-DSS-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-DSS-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-DSS-DES-CBC-SHA Rejected SSLv3 168 bits DES-CBC3-SHA Rejected SSLv3 56 bits DES-CBC-SHA Rejected SSLv3 40 bits EXP-DES-CBC-SHA Rejected SSLv3 128 bits IDEA-CBC-SHA Rejected SSLv3 40 bits EXP-RC2-CBC-MD5 Rejected SSLv3 128 bits RC4-SHA Rejected SSLv3 128 bits RC4-MD5 Rejected SSLv3 40 bits EXP-RC4-MD5 Rejected SSLv3 0 bits NULL-SHA Rejected SSLv3 0 bits NULL-MD5 Rejected TLSv1 256 bits ADH-AES256-SHA Rejected TLSv1 256 bits DHE-RSA-AES256-SHA Rejected TLSv1 256 bits DHE-DSS-AES256-SHA			
2.4.7.5	Insecure and unauthenticated application layer protocols (such as TELNET, FTP, HTTP, SMTP and NTP < v4) are not used.	1 and above	M	TBD in future release
	PASS: No insecure protocols were found			
2.4.7.6	All the products' unused ports are closed, and the minimal required number of ports are active.	1 and above	M	TBD in future release
	FAIL: Too many ports were found open:			

| | ```
Starting Nmap 6.40 ( http://nmap.org ) at 2018-07-13 00:56 GMT Daylight Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.113
Host is up (0.022s latency).
Not shown: 65525 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
6223/tcp open  unknown
6224/tcp open  unknown
6225/tcp open  unknown
6226/tcp open  unknown
6323/tcp open  unknown
6324/tcp open  unknown
6325/tcp open  unknown
6326/tcp open  unknown
8101/tcp open  unknown
8201/tcp open  trivnet2
MAC Address: B8:27:EB:35:A0:B5 (Raspberry Pi Foundation)
```<br>```
Starting Nmap 6.40 ( http://nmap.org ) at 2018-07-13 03:50 GMT Daylight Time
Nmap scan report for 192.168.0.113
Host is up (0.0037s latency).
Not shown: 994 closed ports
PORT       STATE         SERVICE
123/udp    open          ntp
3702/udp   open|filtered ws-discovery
5353/udp   open          zeroconf
10000/udp open|filtered ndmp
19489/udp open|filtered unknown
25546/udp open|filtered unknown
MAC Address: B8:27:EB:35:A0:B5 (Raspberry Pi Foundation)

Nmap done: 1 IP address (1 host up) scanned in 1164.87 seconds
```<br>[redacted] | | | |
| **2.4.7.7** | If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device and is not derived e.g. from serial numbers. Examples are WIFI access passwords and Bluetooth PINs. | 1 and above | M | TBD in future release |
| | N/A:<br>connection authentication was not used:<br>[redacted]<br>[redacted] HTTP/1.1<br>```
Host: 192.168.0.113:8201
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:61.0) Gecko/20100101 Firefox/61.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-None-Match: "4783756a9488092919f640d725022228eb167563"
Cache-Control: max-age=0
```<br>[redacted] | | | |
2.4.7.8	Where a wireless communications interface requires an initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret. For example, Bluetooth Numeric Comparison.	1 and above	M	TBD in future release
	N/A: No pairing process was found to be used.			
2.4.7.9	Where a wireless interface has an initial pairing process, the passkeys are changed from the	1 and above	M	TBD in future
```

	factory issued or reset password prior to providing normal service			release
	N/A: No pairing process was found to be used.			
2.4.7.10	For any WIFI connection, WPA2 with AES or a similar strength encryption has been used and insecure protocols such as WPA and TKIP are disabled.	1 and above	M	TBD in future release
	N/A - **FAIL:** Initially the XXX hub acts as an open access point, and broadcasts itself waiting for connections.  The XXX hub then pairs itself as a client, with a Wi-Fi router using the available protocols on the router.			
2.4.7.11	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	1 and above	M	TBD in future release
	N/A: The XXX device does not act as a Wi-Fi hub/router			
2.4.7.12	All network communications keys are stored securely, in accordance with industry standards such as FIPS 140 [ref 5] or similar.	1 and above	M	TBD in future release
	PASS: The XXX stores its keys, on a drive encrypted with a strong passphrase.			
2.4.7.13	Where the MQTT protocol is used, it is protected by a TLS connection with no known cipher vulnerabilities.	1 and above	M	TBD in future release
	N/A: The MQTT protocol was not used.			
2.4.7.14	Where the CoAP protocol is used, it is protected by a DTLS connection with no known cipher vulnerabilities.	1 and above	M	TBD in future release
	N/A: The CoAP protocol was not used.			
2.4.7.15	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A [ref 2] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	1 and above	M	TBD in future release
	PASS: No insecure SSL protocols were found to be used:			

```
Testing SSL server 192.168.0.113 on port 8101

  Supported Server Cipher(s):
    Failed     SSLv2  168 bits  DES-CBC3-MD5
    Failed     SSLv2   56 bits  DES-CBC-MD5
    Failed     SSLv2  128 bits  IDEA-CBC-MD5
    Failed     SSLv2   40 bits  EXP-RC2-CBC-MD5
    Failed     SSLv2  128 bits  RC2-CBC-MD5
    Failed     SSLv2   40 bits  EXP-RC4-MD5
    Failed     SSLv2  128 bits  RC4-MD5
    Rejected   SSLv3  256 bits  ADH-AES256-SHA
    Rejected   SSLv3  256 bits  DHE-RSA-AES256-SHA
    Rejected   SSLv3  256 bits  DHE-DSS-AES256-SHA
    Rejected   SSLv3  256 bits  AES256-SHA
    Rejected   SSLv3  128 bits  ADH-AES128-SHA
    Rejected   SSLv3  128 bits  DHE-RSA-AES128-SHA
    Rejected   SSLv3  128 bits  DHE-DSS-AES128-SHA
    Rejected   SSLv3  128 bits  AES128-SHA
    Rejected   SSLv3  168 bits  ADH-DES-CBC3-SHA
    Rejected   SSLv3   56 bits  ADH-DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-ADH-DES-CBC-SHA
    Rejected   SSLv3  128 bits  ADH-RC4-MD5
    Rejected   SSLv3   40 bits  EXP-ADH-RC4-MD5
    Rejected   SSLv3  168 bits  EDH-RSA-DES-CBC3-SHA
    Rejected   SSLv3   56 bits  EDH-RSA-DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-EDH-RSA-DES-CBC-SHA
    Rejected   SSLv3  168 bits  EDH-DSS-DES-CBC3-SHA
    Rejected   SSLv3   56 bits  EDH-DSS-DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-EDH-DSS-DES-CBC-SHA
    Rejected   SSLv3  168 bits  DES-CBC3-SHA
    Rejected   SSLv3   56 bits  DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-DES-CBC-SHA
    Rejected   SSLv3  128 bits  IDEA-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-RC2-CBC-MD5
    Rejected   SSLv3  128 bits  RC4-SHA
    Rejected   SSLv3  128 bits  RC4-MD5
    Rejected   SSLv3   40 bits  EXP-RC4-MD5
    Rejected   SSLv3    0 bits  NULL-SHA
    Rejected   SSLv3    0 bits  NULL-MD5
    Rejected   TLSv1  256 bits  ADH-AES256-SHA
    Rejected   TLSv1  256 bits  DHE-RSA-AES256-SHA
    Rejected   TLSv1  256 bits  DHE-DSS-AES256-SHA
    Rejected   TLSv1  256 bits  AES256-SHA
    Rejected   TLSv1  128 bits  ADH-AES128-SHA
    Rejected   TLSv1  128 bits  DHE-RSA-AES128-SHA
    Rejected   TLSv1  128 bits  DHE-DSS-AES128-SHA
    Rejected   TLSv1  128 bits  AES128-SHA
    Rejected   TLSv1  168 bits  ADH-DES-CBC3-SHA
    Rejected   TLSv1   56 bits  ADH-DES-CBC-SHA
    Rejected   TLSv1   40 bits  EXP-ADH-DES-CBC-SHA
```

	 Testing SSL server 192.168.0.113 on port 8201 Supported Server Cipher(s): Failed SSLv2 168 bits DES-CBC3-MD5 Failed SSLv2 56 bits DES-CBC-MD5 Failed SSLv2 128 bits IDEA-CBC-MD5 Failed SSLv2 40 bits EXP-RC2-CBC-MD5 Failed SSLv2 128 bits RC2-CBC-MD5 Failed SSLv2 40 bits EXP-RC4-MD5 Failed SSLv2 128 bits RC4-MD5 Rejected SSLv3 256 bits ADH-AES256-SHA Rejected SSLv3 256 bits DHE-RSA-AES256-SHA Rejected SSLv3 256 bits DHE-DSS-AES256-SHA Rejected SSLv3 256 bits AES256-SHA Rejected SSLv3 128 bits ADH-AES128-SHA Rejected SSLv3 128 bits DHE-RSA-AES128-SHA Rejected SSLv3 128 bits DHE-DSS-AES128-SHA Rejected SSLv3 128 bits AES128-SHA Rejected SSLv3 168 bits ADH-DES-CBC3-SHA Rejected SSLv3 56 bits ADH-DES-CBC-SHA Rejected SSLv3 40 bits EXP-ADH-DES-CBC-SHA Rejected SSLv3 128 bits ADH-RC4-MD5 Rejected SSLv3 40 bits EXP-ADH-RC4-MD5 Rejected SSLv3 168 bits EDH-RSA-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-RSA-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA Rejected SSLv3 168 bits EDH-DSS-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-DSS-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-DSS-DES-CBC-SHA Rejected SSLv3 168 bits DES-CBC3-SHA Rejected SSLv3 56 bits DES-CBC-SHA Rejected SSLv3 40 bits EXP-DES-CBC-SHA Rejected SSLv3 128 bits IDEA-CBC-SHA Rejected SSLv3 40 bits EXP-RC2-CBC-MD5 Rejected SSLv3 128 bits RC4-SHA Rejected SSLv3 128 bits RC4-MD5 Rejected SSLv3 40 bits EXP-RC4-MD5 Rejected SSLv3 0 bits NULL-SHA Rejected SSLv3 0 bits NULL-MD5 Rejected TLSv1 256 bits ADH-AES256-SHA Rejected TLSv1 256 bits DHE-RSA-AES256-SHA Rejected TLSv1 256 bits DHE-DSS-AES256-SHA			
2.4.7.16	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	1 and above	M	TBD in future release
	PASS: Legitimate UK SSL protocols used. Uncertain of other territories XXX devices are sold in.			

```
Testing SSL server 192.168.0.113 on port 8101

  Supported Server Cipher(s):
    Failed     SSLv2  168 bits  DES-CBC3-MD5
    Failed     SSLv2   56 bits  DES-CBC-MD5
    Failed     SSLv2  128 bits  IDEA-CBC-MD5
    Failed     SSLv2   40 bits  EXP-RC2-CBC-MD5
    Failed     SSLv2  128 bits  RC2-CBC-MD5
    Failed     SSLv2   40 bits  EXP-RC4-MD5
    Failed     SSLv2  128 bits  RC4-MD5
    Rejected   SSLv3  256 bits  ADH-AES256-SHA
    Rejected   SSLv3  256 bits  DHE-RSA-AES256-SHA
    Rejected   SSLv3  256 bits  DHE-DSS-AES256-SHA
    Rejected   SSLv3  256 bits  AES256-SHA
    Rejected   SSLv3  128 bits  ADH-AES128-SHA
    Rejected   SSLv3  128 bits  DHE-RSA-AES128-SHA
    Rejected   SSLv3  128 bits  DHE-DSS-AES128-SHA
    Rejected   SSLv3  128 bits  AES128-SHA
    Rejected   SSLv3  168 bits  ADH-DES-CBC3-SHA
    Rejected   SSLv3   56 bits  ADH-DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-ADH-DES-CBC-SHA
    Rejected   SSLv3  128 bits  ADH-RC4-MD5
    Rejected   SSLv3   40 bits  EXP-ADH-RC4-MD5
    Rejected   SSLv3  168 bits  EDH-RSA-DES-CBC3-SHA
    Rejected   SSLv3   56 bits  EDH-RSA-DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-EDH-RSA-DES-CBC-SHA
    Rejected   SSLv3  168 bits  EDH-DSS-DES-CBC3-SHA
    Rejected   SSLv3   56 bits  EDH-DSS-DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-EDH-DSS-DES-CBC-SHA
    Rejected   SSLv3  168 bits  DES-CBC3-SHA
    Rejected   SSLv3   56 bits  DES-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-DES-CBC-SHA
    Rejected   SSLv3  128 bits  IDEA-CBC-SHA
    Rejected   SSLv3   40 bits  EXP-RC2-CBC-MD5
    Rejected   SSLv3  128 bits  RC4-SHA
    Rejected   SSLv3  128 bits  RC4-MD5
    Rejected   SSLv3   40 bits  EXP-RC4-MD5
    Rejected   SSLv3    0 bits  NULL-SHA
    Rejected   SSLv3    0 bits  NULL-MD5
    Rejected   TLSv1  256 bits  ADH-AES256-SHA
    Rejected   TLSv1  256 bits  DHE-RSA-AES256-SHA
    Rejected   TLSv1  256 bits  DHE-DSS-AES256-SHA
    Rejected   TLSv1  256 bits  AES256-SHA
    Rejected   TLSv1  128 bits  ADH-AES128-SHA
    Rejected   TLSv1  128 bits  DHE-RSA-AES128-SHA
    Rejected   TLSv1  128 bits  DHE-DSS-AES128-SHA
    Rejected   TLSv1  128 bits  AES128-SHA
    Rejected   TLSv1  168 bits  ADH-DES-CBC3-SHA
    Rejected   TLSv1   56 bits  ADH-DES-CBC-SHA
    Rejected   TLSv1   40 bits  EXP-ADH-DES-CBC-SHA
```

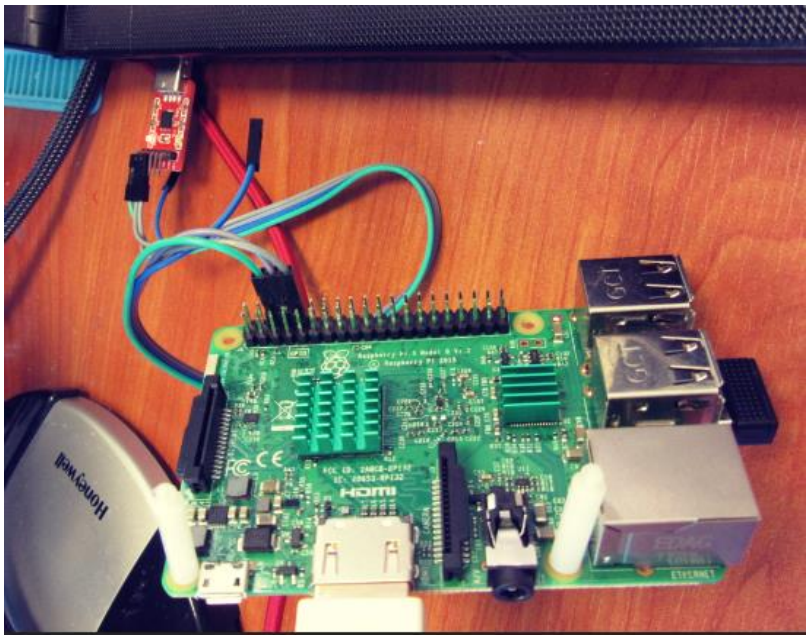
	Testing SSL server 192.168.0.113 on port 8201 Supported Server Cipher(s): Failed SSLv2 168 bits DES-CBC3-MD5 Failed SSLv2 56 bits DES-CBC-MD5 Failed SSLv2 128 bits IDEA-CBC-MD5 Failed SSLv2 40 bits EXP-RC2-CBC-MD5 Failed SSLv2 128 bits RC2-CBC-MD5 Failed SSLv2 40 bits EXP-RC4-MD5 Failed SSLv2 128 bits RC4-MD5 Rejected SSLv3 256 bits ADH-AES256-SHA Rejected SSLv3 256 bits DHE-RSA-AES256-SHA Rejected SSLv3 256 bits DHE-DSS-AES256-SHA Rejected SSLv3 256 bits AES256-SHA Rejected SSLv3 128 bits ADH-AES128-SHA Rejected SSLv3 128 bits DHE-RSA-AES128-SHA Rejected SSLv3 128 bits DHE-DSS-AES128-SHA Rejected SSLv3 128 bits AES128-SHA Rejected SSLv3 168 bits ADH-DES-CBC3-SHA Rejected SSLv3 56 bits ADH-DES-CBC-SHA Rejected SSLv3 40 bits EXP-ADH-DES-CBC-SHA Rejected SSLv3 128 bits ADH-RC4-MD5 Rejected SSLv3 40 bits EXP-ADH-RC4-MD5 Rejected SSLv3 168 bits EDH-RSA-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-RSA-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA Rejected SSLv3 168 bits EDH-DSS-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-DSS-DES-CBC-SHA Rejected SSLv3 40 bits EXP-EDH-DSS-DES-CBC-SHA Rejected SSLv3 168 bits DES-CBC3-SHA Rejected SSLv3 56 bits DES-CBC-SHA Rejected SSLv3 40 bits EXP-DES-CBC-SHA Rejected SSLv3 128 bits IDEA-CBC-SHA Rejected SSLv3 40 bits EXP-RC2-CBC-MD5 Rejected SSLv3 128 bits RC4-SHA Rejected SSLv3 128 bits RC4-MD5 Rejected SSLv3 40 bits EXP-RC4-MD5 Rejected SSLv3 0 bits NULL-SHA Rejected SSLv3 0 bits NULL-MD5 Rejected TLSv1 256 bits ADH-AES256-SHA Rejected TLSv1 256 bits DHE-RSA-AES256-SHA Rejected TLSv1 256 bits DHE-DSS-AES256-SHA			
2.4.7.18	The product only enables the communications interfaces, network protocols, application protocols and network services necessary for the products' operation.	1 and above	M	TBD in future release
	FAIL: Primary communications channel used port 8201, port 22 (SSH) was also open: Starting Nmap 6.40 (http://nmap.org) at 2018-07-13 00:56 GMT Daylight Time mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers Nmap scan report for 192.168.0.113 Host is up (0.022s latency). Not shown: 65525 closed ports PORT STATE SERVICE 22/tcp open ssh 6223/tcp open unknown 6224/tcp open unknown 6225/tcp open unknown 6226/tcp open unknown 6323/tcp open unknown 6324/tcp open unknown 6325/tcp open unknown 6326/tcp open unknown 8101/tcp open unknown 8201/tcp open trivnet2 MAC Address: B8:27:EB:35:A0:B5 (Raspberry Pi Foundation)			

	Starting Nmap 6.40 (http://nmap.org) at 2018-07-13 03:50 GMT Daylight Time Nmap scan report for 192.168.0.113 Host is up (0.0037s latency). Not shown: 994 closed ports PORT STATE SERVICE 123/udp open ntp 3702/udp open|filtered ws-discovery 5353/udp open zeroconf 10000/udp open|filtered ndmp 19489/udp open|filtered unknown 25546/udp open|filtered unknown MAC Address: B8:27:EB:35:A0:B5 (Raspberry Pi Foundation) Nmap done: 1 IP address (1 host up) scanned in 1164.87 seconds			
2.4.7.19	Communications protocols should be at the most secure versions available and/or appropriate for the product. For example, Bluetooth 4.2 rather than 4.0.	1 and above	M	TBD in future release
	N/A: The device starts as an open access point.			
2.4.7.20	Post product launch communications protocols should be maintained to the most secure versions available and/or appropriate for the product.	1 and above	M	TBD in future release
	FAIL: Communications to the cloud server “app-xxx.com” used outdated TSL1.0 protocol. “sslscan app-xxx.com” Supported Server Cipher(s): Preferred TLSv1.2 128 bits ECDHE-RSA-AES128 Accepted TLSv1.2 256 bits ECDHE-RSA-AES256 Accepted TLSv1.2 128 bits ECDHE-RSA-AES128 Accepted TLSv1.2 256 bits ECDHE-RSA-AES256 Accepted TLSv1.2 128 bits AES128-GCM-SHA25 Accepted TLSv1.2 256 bits AES256-GCM-SHA38 Accepted TLSv1.2 128 bits AES128-SHA Accepted TLSv1.2 256 bits AES256-SHA Accepted TLSv1.2 112 bits DES-CBC3-SHA Preferred TLSv1.1 128 bits ECDHE-RSA-AES128 Accepted TLSv1.1 256 bits ECDHE-RSA-AES256 Accepted TLSv1.1 128 bits AES128-SHA Accepted TLSv1.1 256 bits AES256-SHA Accepted TLSv1.1 112 bits DES-CBC3-SHA Preferred TLSv1.0 128 bits ECDHE-RSA-AES128 Accepted TLSv1.0 256 bits ECDHE-RSA-AES256 Accepted TLSv1.0 128 bits AES128-SHA Accepted TLSv1.0 256 bits AES256-SHA Accepted TLSv1.0 112 bits DES-CBC3-SHA			
2.4.7.21	If a factory reset is made, the device should warn that secure operation may be compromised unless updated.	1 and above	M	TBD in future release
	N/A: No factory reset mechanism was discovered.			

Internal analysis

Internal interfaces, USB, Serial, JTAG SPI

Hardware tools: Bash Bunny, JTAGulator, J-LINK, Picoscope, SPI Programmer, Microscope
Software tools: N/A

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.4.5	Any debug interface (for example, I/O ports such as JTAG) only communicates with authorised and authenticated entities on the production devices. (Is secured on the production devices.)	1 and above	M	TBD in future release
	PASS: The Raspberry Pi's motherboard (Used by XXX) serial port was found to be disabled. The Raspberry PI JTAG interface by default is difficult to access: 			
2.4.4.6	The hardware incorporates protection against tampering, and this has been enabled.	1 and above	M	TBD in future release
	FAIL: No sign of protection against tampering.			
2.4.4.9	All communications port(s), such as USB, RS232 etc., which are not used as part of the product's normal operation are not physically accessible or only communicate with authorised and authenticated	1 and above	A	TBD in future release

	entities.			
	FAIL: Plugging a USB keyboard into the USB port is recognised, during boot.			

```
[    2.482207] NET: Registered protocol family 38
[    2.491640] usb 1-1: New USB device found, idVendor=0424, idProduct=9514
[    2.503719] usb 1-1: New USB device strings: Mfr=0, Product=0, SerialNumber=0
[    2.517098] hub 1-1:1.0: USB hub found
[    2.526393] hub 1-1:1.0: 5 ports detected
[    2.812433] usb 1-1.1: new high-speed USB device number 3 using dwc_otg
[    2.922673] usb 1-1.1: New USB device found, idVendor=0424, idProduct=ec00
[    2.934203] usb 1-1.1: New USB device strings: Mfr=0, Product=0, SerialNumber
=0
[    2.948884] smsc95xx v1.0.4
[    3.015284] smsc95xx 1-1.1:1.0 eth0: register 'smsc95xx' at usb-3f980000.usb-
1.1, smsc95xx USB 2.0 Ethernet, b8:27:eb:aa:b2:cf
[    3.262428] usb 1-1.3: new full-speed USB device number 4 using dwc_otg
[    3.382139] usb 1-1.3: New USB device found, idVendor=1997, idProduct=2433
[    3.393879] usb 1-1.3: New USB device strings: Mfr=1, Product=2, SerialNumber
=0
[    3.406053] usb 1-1.3: Product: Mini Keyboard
[    3.415198] usb 1-1.3: Manufacturer:
[    3.430013] input:   Mini Keyboard as /devices/platform/soc/3f980000.usb/usb1
/1-1/1-1.3/1-1.3:1.0/0003:1997:2433.0001/input/input0
[    3.502640] hid-generic 0003:1997:2433.0001: input,hidraw0: USB HID v1.01 Key
board [  Mini Keyboard] on usb-3f980000.usb-1.3/input0
[    3.525877] input:   Mini Keyboard as /devices/platform/soc/3f980000.usb/usb1
/1-1/1-1.3/1-1.3:1.1/0003:1997:2433.0002/input/input1
```

3) Embedded device – Gaining shell access

Ethernet Exploitation
Protocol implementation weakness.

Wireless Exploitation
HackRF, KillerBee, Ubertooth

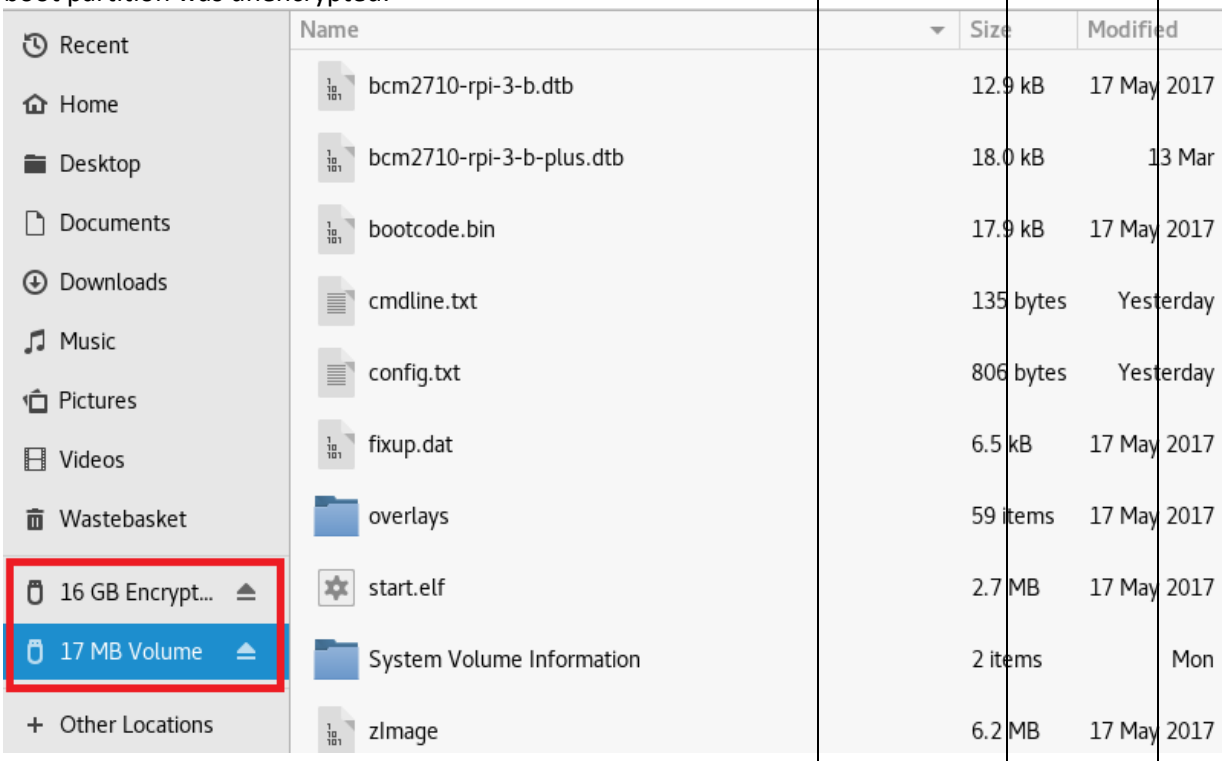
USB exploitation
PoisonTap, BashBunny and Facedancer21

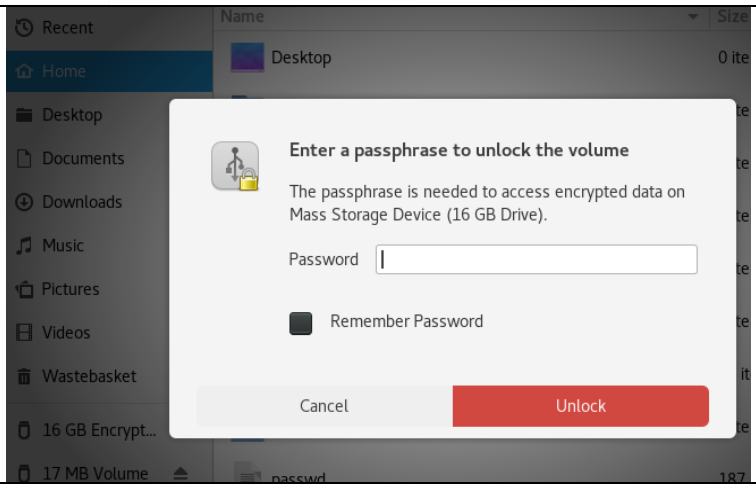
UART exploitation
Identifying the connections, identifying the baud rate, interacting with the device to gain a shell

I2C/SPI exploitation
Identifying the connections, reading writing to the EEPROM

JTAG exploitation
Identifying the connections, reading writing to the EEPROM. Reading memory contents. Analysing binaries.

Technique	Description
Ethernet Exploitation	Protocol implementation weakness using Dedsploit. Use Nessus, Nmap with vulscan to identify vulnerable services. V3nom MetaSploit.
Wireless Exploitation	BLE Sniffer, HackRF, LimeSDR, KillerBee, OpenSniffer, Ubertooth, Wi-Fi Pineapple Tetra using Wireshark and Universal Radio Hacker to carry out wireless attacks.
USB exploitation	Using BashBunny/Poisontap and Facedancer21 to carry out low level USB fuzzing using UMAP.
UART exploitation	Identifying the connections using JTAGulator/Picoscope, then identifying the band rate using Picoscope and baudrate.py to interact with the device with the intent to gain a shell.
I2C/SPI exploitation	Identifying the connections using JTAGulator/Picoscope, then reading/writing to the EEPROM using a SPI programmer. Analysing binaries using binwalk, IDAPRO, and firmwalker.
I2C/SPI exploitation	BLE Sniffer, HackRF, LimeSDR, KillerBee, OpenSniffer, Ubertooth, Wi-Fi Pineapple Tetra using Wireshark and Universal Radio Hacker to carry out wireless attacks.
JTAG exploitation	Identifying the connections using JTAGulator/Picoscope, reading/writing to the EEPROM. Reading memory contents. Analysing binaries using binwalk, IDAPRO, and firmwalker.
Wireless Exploitation	BLE Sniffer, HackRF, LimeSDR, KillerBee, OpenSniffer, Ubertooth, Wi-Fi Pineapple Tetra using Wireshark and Universal Radio Hacker to carry out wireless attacks.

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.4.13	In production devices, the microcontroller/ microprocessor(s) shall not allow the firmware to be read out of the products non-volatile [FLASH] memory or where a separate non-volatile memory device is used the contents shall be encrypted.	1 and above	M	TBD in future release
	FAIL: Only one partition on microSD card was encrypted, the other the boot partition was unencrypted:  			
2.4.4.14	Where the products' credential/key storage is external to its processor, the storage and processor shall be cryptographically paired in such a way to prevent the credential/key storage being used by unauthorised software.	1 and above	M	TBD in future release
	FAIL: Storage was accessible by another computer, which when accessed asked for a passphrase.			

	 Recent Home Desktop Documents Downloads Music Pictures Videos Wastebasket 16 GB Encrypt... 17 MB Volume Name Size Desktop 0 ite Enter a passphrase to unlock the volume The passphrase is needed to access encrypted data on Mass Storage Device (16 GB Drive). Password Remember Password Cancel Unlock				

4) Embedded device – Firmware analysis

From a security perspective firmware is the most critical component of an embedded device. Firmware resides on the non-volatile section of the device, allowing and enabling the device to perform different tasks required for the functioning of the device.

Technique	Description
Obtaining the firmware	Downloading from the Internet.
Extracting from the device	I2C/SPI exploitation Identifying the connections using JTAGulator/Picoscope, then reading/writing from/to the EEPROM using a SPI programmer. Analysing binaries using binwalk, IDAPRO, and firmwalker. JTAG exploitation Identifying the connections using JTAGulator/Picoscope, reading/writing to the EEPROM. Reading memory contents. Analysing binaries using binwalk, IDAPRO, and firmwalker.
Reversing applications	Analysing binaries using binwalk, IDAPRO, and firmwalker.
Extracting firmware.	Manual method. Automated method – binwalk.
Looking for hardcoded secrets.	Firmwalker. Credentials, backdoor, sensitive URLS, access tokens, local pathnames.

5) Embedded device – Backdooring the firmware

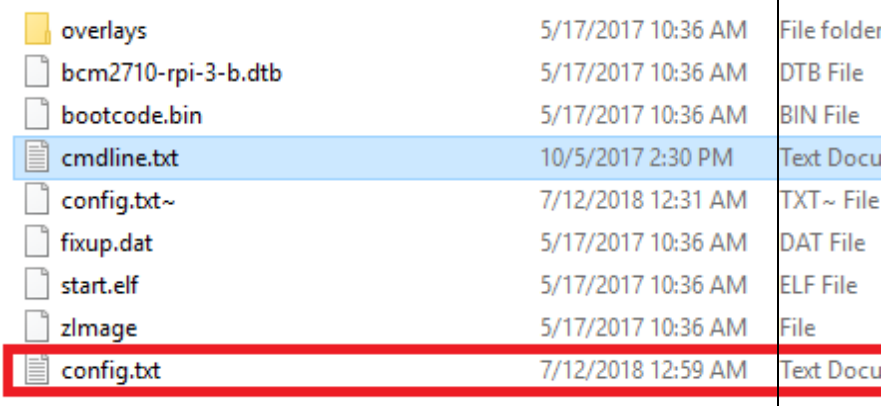
Backdooring the firmware is one of the main security issues which devices faces, if it has no secure integrity checks and signature validation.

Req. No.	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.5.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/ or sandbox.	1 and above	M	TBD in future release
	FAIL: It was possible to load new files on the boot partition and change the boot configuration for example to enable the serial port. overlays 5/17/2017 10:36 AM File folder bcm2710-rpi-3-b.dtb 5/17/2017 10:36 AM DTB File bootcode.bin 5/17/2017 10:36 AM BIN File cmdline.txt 10/5/2017 2:30 PM Text Docu config.txt~ 7/12/2018 12:31 AM TXT~ File fixup.dat 5/17/2017 10:36 AM DAT File start.elf 5/17/2017 10:36 AM ELF File zImage 5/17/2017 10:36 AM File config.txt 7/12/2018 12:59 AM Text Docu			
2.4.5.2	Where remote software upgrade can be supported by the device, the software images are digitally signed by the organisation's approved signing authority.	1 and above	M	TBD in future release
	N/A: Unable to test as the device was already registered.			
2.4.5.3	A software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.	1 and above	M	TBD in future release
	N/A: Unable to test as the device was already registered.			
2.4.5.7	The product's software signing root of trust is stored in tamper-resistant memory.	1 and above	M	TBD in future release
	N/A: Unable to test, as devices drive was encrypted with a strong passphrase			
2.4.4.1	Where production devices have a CPU watchdog, it is enabled	1 and above	M	TBD in

5	and will reset the device in the event of any unauthorised attempts to pause or suspend the CPU's execution.			future release
	N/A: Unable to test, as could not easily gain access to the JTAG interface			
2.4.5.28	Where a device doesn't support Secure Boot, user data and secrets must be erased when a firmware update is installed.	1 and above	M	TBD in future release
	N/A: Unable to test as the device was already registered.			
2.4.5.29	Where a device cannot verify authenticity of updates itself (e.g. due to no cryptographic capabilities), only local update by a physically present user is permitted.	1 and above	M	TBD in future release
	N/A unable to test, as could find no mechanism for update as device was already registered.			
2.4.5.30	When a device cannot verify authenticity of updates itself, a mechanism for the user to verify update authenticity out-of-band must be provided.	1 and above	M	TBD in future release
	N/A: Unable to test as the device was already registered.			
2.4.5.31	Cryptographic keys for update integrity protection and confidentiality are securely managed in accordance with industry standards such as FIPS 140 [ref 5].	1 and above	M	TBD in future release
	PASS: The XXX drive where the cryptographic keys are stored, is encrypted with a strong passphrase.			
2.4.5.32	There is secure provisioning of cryptographic keys for updates during manufacture in accordance with industry standards such as FIPS 140 [ref 5].	1 and above	M	TBD in future release
	N/A: Unable to test as the device was already registered.			

6) Firmware, software and applications - Auditing the file system and programs in use

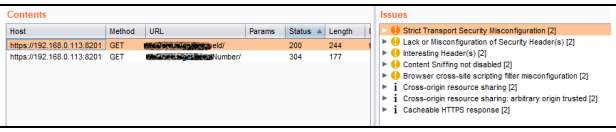
Operating system audit
Nessus Professional audit

Req. No.	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.4.1	The product's processor system has an irrevocable Secure Boot process.	1 and above	A	TBD in future release
	FAIL: It was possible to modify boot files to enable serial connectivity.  overlays 5/17/2017 10:36 AM File folder bcm2710-rpi-3-b.dtb 5/17/2017 10:36 AM DTB File bootcode.bin 5/17/2017 10:36 AM BIN File cmdline.txt 10/5/2017 2:30 PM Text Docu config.txt~ 7/12/2018 12:31 AM TXT~ File fixup.dat 5/17/2017 10:36 AM DAT File start.elf 5/17/2017 10:36 AM ELF File zImage 5/17/2017 10:36 AM File config.txt 7/12/2018 12:59 AM Text Docu			
2.4.4.4	The secure boot process is enabled by default.	1 and above	A	TBD in future release
	FAIL: It was possible to modify boot files to enable serial connectivity.			
2.4.5.6	Where production devices have a CPU watchdog, it is enabled and will reset the device in the event of any unauthorised attempts to pause or suspend the CPU's execution.	1 and above	M	TBD in future release
	NA: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.5.15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example, security related processes should be executed at higher privilege levels in the application processor hardware.	1 and above	M	TBD in future release
	NA: Unable to test as was unable to obtain shell access.			
2.4.6.5	Password file(s) are owned by and are only accessible to and writable by the Devices' OS's most privileged account.	1 and above	M	TBD in future

				release
	NA: Unable to test as was unable to obtain shell access			
2.4.6.10	All the applicable security features supported by the OS are enabled.	1 and above	M	TBD in future release
	FAIL: Linux secure boot was not enabled.			
2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is unique to each device in the product family.	1 and above	M	TBD in future release
	N/A: User sets their username/password on the first boot of the device. POST /prod/register_hub HTTP/1.1 Host: [redacted] Content-Type: application/json Connection: close Accept: */* User-Agent: [redacted]twork/808.3 Darwin/16.3.0 Content-Length: 87 Accept-Language: en-gb Accept-Encoding: gzip, deflate {"mac_addr":"b8-27-eb-60-f5-e0","password":"PasswOrd","email":"pcutest@procheckup.com"}			
2.4.8.4	The product does not accept the use of null or blank passwords.	1 and above	M	TBD in future release
	FAIL: Queries to the devices API was not protected by password or credentials. https://192.168.0.113:8201/xxxx/getSerialNumber/ GET [redacted]etSerialNumber/ HTTP/1.1 Host: 192.168.0.113:8201 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Upgrade-Insecure-Requests: 1 If-None-Match: "4783756a9488092919f640d725022228eb167563" Cache-Control: max-age=0			
2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	1 and above	M	TBD in future release
	N/A: Unable to test further as device was already registered.			
2.4.8.6	The product/system enforces passwords to be compliant as NIST SP800-63b [ref 26] or similar recommendations on: password length; characters from the groupings and special characters.	1 and above	M	TBD in future release
	FAIL: The password required had complexity requirements including mixed alphanumeric and 8 characters - though not special characters.			

	POST /prod/register_hub HTTP/1.1 Host:[redacted] Content-Type: application/json Connection: close Accept: */* User-Agent:[redacted]etwork/808.3 Darwin/16.3.0 Content-Length: 87 Accept-Language: en-gb Accept-Encoding: gzip, deflate {"mac_addr":"b8-27-eb-60-f5-e0","password":"PasswOrd","email":"pcutest@procheckup.com"}			
2.4.8.7	The product has defence against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	1 and above	M	TBD in future release
	N/A: Unable to test further as device was already registered.			
2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard such as NIST SP800-63b [ref 26] or similar.	1 and above	M	TBD in future release
	N/A: Unable to test as unable to obtain shell access, also the device drive was encrypted, and password protected.			
2.4.8.9	The product supports access control measures to the root account to restrict access to sensitive information or system processes.	1 and above	M	TBD in future release
	N/A: Unable to test as unable to obtain shell access, also the device drive was encrypted, and password protected.			
2.4.8.11	The product only allows controlled user account access; access using anonymous or guest user accounts are not supported without justification.	1 and above	M	TBD in future release
	PASS: Only registered accounts were allowed access.			
2.4.8.13	The product supports having any or all the factory default user login passwords, altered prior to normal service. This is to avoid the type of attacks where factory default logins and passwords are published on the web, which allows attackers to mount very simple scanning and dictionary attacks on devices.	1 and above	M	TBD in future release
	N/A: Unable to test as could not determine if a factory reset mechanism existed.			
2.4.8.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorised party.	1 and above	M	TBD in future release
	N/A: Unable to test as could not determine if a factory reset mechanism existed.			

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.10.6	Do not store passwords in user stores in plain text. Use strong passwords and incorporate a random salt value with the password.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement. The device did not support a web interface, only an API.			
2.4.10.9	A vulnerability assessment has been performed before deployment and on an ongoing basis afterwards.	1 and above	M	TBD in future release
	N/A: This seems to be a function of audit.			
2.4.10.12	All inputs and outputs are validated using for example a whitelist containing authorised origins of data and valid attributes of such data.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement. The device did not support a web interface, only an API.			
2.4.10.13	Secure Administration Interfaces: It is important that configuration management functionality is accessible only by authorised operators and administrators. Enforce Strong Authentication over administration interfaces, for example, by using certificates.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement. The device did not support a web interface, only an API.			
2.4.10.14	Reduce the lifetime of sessions to mitigate the risk of session hijacking and replay attacks. The shorter the session, the less time an attacker has to capture a session cookie and use it to access an application.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement. The device did not support a web interface, only an API.			
2.4.10.15	All inputs and outputs are checked for validity. E.g. “Fuzzing” tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli.	1 and above	M	TBD in future release
	PASS: The available API calls on the device successfully passed fuzzing by BURP.			

Web interface audit

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Web Systems.
Software tools: BurpSuite, Acunetix

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.10.2	Where the product or service provides a web-based interface, public and restricted areas shall be separated for authentication.	1 and above	M	TBD in future release
	N/A: No web interface was provided by the device.			
2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family	1 and above	M	TBD in future release
	N/A: No web interface was provided by the device.			
2.4.10.5	The web user interface is protected by automatic session/logout timeout function.	1 and above	M	TBD in future release
	N/A: No web interface was provided by the device.			
2.4.10.7	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	1 and above	M	TBD in future release
	N/A: No web interface was provided by the device.			
2.4.10.8	The web user interface shall follow good practice guidelines, such as those listed in the OWASP (https://www.owasp.org) top 10 attacks.	1 and above	M	TBD in future release
	N/A: No web interface was provided by the device.			
2.4.10.10	All data being transferred over interfaces should be validated where	1 and above	M	TBD in future release

	appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency			
	PASS: During limited testing the API performed character validation.			
2.4.10.11	Sanitise input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script.	1 and above	M	TBD in future release
	N/A: No web interface was provided by the device.			

Mobile application tests

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.11.1	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement.			
2.4.11.3	The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access. Upon detection of tampering of the databases or files they are re-initialised.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement.			
2.4.11.4	Where the application communicates with a product related remote server(s) or device it does so over a secure connection such as a TLS connection using certificate pinning.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed,			

	which were out of scope of this engagement.			
2.4.11.5	The product securely stores any passwords using an industry standard cryptographic algorithm, for example see FIPS 140-2 [ref 5].	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement.			
2.4.11.6	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement.			
2.4.11.7	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	1 and above	M	TBD in future release
	N/A: Android and iOS clients existed, which were out of scope of this engagement.			

Key management audit

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.4.16	Where the product has a hardware source for generating true random numbers, all cryptographic functions shall use this hardware source as the sole source of random numbers and nonces.	1 and above	M	TBD in future release
	NA: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.9.4	There is a secure method of key insertion that protects keys against copying.	1 and above	M	TBD in future release
	NA: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.9.5	All the product related cryptographic functions have no publicly known weaknesses, for example MD5 and SHA-1 are not used, e.g. those stipulated in NIST SP800-131A [ref 2].	1 and above	M	TBD in future release
	NA: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.9.6	All the product related cryptographic functions are sufficiently secure for the lifecycle of the product, e.g. those stipulated in NIST SP800-131A [ref 2].	1 and above	M	TBD in future release
	NA: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.9.7	The product stores all sensitive unencrypted parameters, (e.g. keys), in a secure, tamper resistant location.	1 and above	M	TBD in future release
	PASS: Sensitive data was stored on an encrypted drive.			

Data store audit

Compliance Applicability – Privacy

This section's intended audience is for those personnel who are responsible for Data Protection and Privacy regulatory compliance.

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.12.1	The product/service stores the minimum amount of personal information from users.	1 and above	M	TBD in future release
	N/A: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.12.2	The product/service ensures that all personal user data is encrypted at rest and in transit.	1 and above	M	TBD in future release
	Personally, identifiable e-mail address is sent over a secure link. https://xxxx/prod/register_hub POST /prod/register_hub HTTP/1.1 Host: [redacted]m Content-Type: application/json Connection: close Accept: */* User-Agent: [redacted]FNetwork/808.3 Darwin/16.3.0 Content-Length: 87 Accept-Language: en-gb Accept-Encoding: gzip, deflate {"mac_addr":"b8-27-eb-60-f5-e0","password":"PasswOrd","email":"pcutest@procheckup.com"}			
2.4.12.3	The product/service ensures that only authorised personnel have access to personal data of users.	1 and above	M	TBD in future release
	N/A: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.4.12.4	The product/service ensures that personal data is anonymised whenever possible and in particular in any reporting.	1 and above	M	TBD in future release
	N/A: Unable to test, as we were unable to obtain a shell on device, or easily access the JTAG interface.			
2.3.10.5	The Product Manufacturer or Service Provider shall ensure that a data retention policy is in place, and compliant with the legal requirements for the territories the product or service is deployed.	1 and above	M	TBD in future release
	N/A: Not applicable to this test			
2.4.12.6	There is a method or methods for the product owner to be informed about what Personal Information is collected, why, where it will be stored.	1 and above	M	TBD in future release
	FAIL: No notification on thick client, or guidance within instruction.			

2.4.12.7	There is a method or methods for the product owner to check/verify what Personal Information is collected and deleted.	1 and above	M	TBD in future release
	N/A: Out of the scope of this engagement.			
2.4.12.8	The product/service can be made compliant with the local and/or regional data protection legislation where the product is to be sold.	1 and above	M	TBD in future release
	N/A: Out of the scope of this engagement.			
2.4.12.9	The supplier or manufacturer of any device shall provide information about how the device(s) functions within the end user's network.	1 and above	A	TBD in future release
	FAIL: No such information provided			
2.4.12.10	The supplier or manufacturer of any devices or devices shall provide information about how the device(s) shall be setup to maintain the end user's privacy and security.	1 and above	M	TBD in future release
	FAIL: No such information provided			
2.4.12.11	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal shall be carried out to maintain the end user's privacy and security.	1 and above	M	TBD in future release
	FAIL: No such information provided			
2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	1 and above	M	TBD in future release
	FAIL: No such information provided			
2.4.12.13	Devices and services should be designed with security usability in mind, reducing where possible, security friction and decision points that may have a detrimental impact on security. Best practices on usable security should be followed, particularly for user interaction and user interfaces.	1 and above	M	TBD in future release
	PASS: The basics of security usability are in place.			

Cloud and supporting network audit

This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Cloud or Network Systems.
Software tools: BURPSuite Pro, Nessus Pro

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	1 and above	M	TBD in future release
	PASS: Both cloud servers had their server banners disabled. https://app-xxx.com/a HTTP/1.1 204 No Content Date: Wed, 25 Jul 2018 01:55:28 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, no-store, must-revalidate Content-Type: image/gif Server: Golfe2 Content-Length: 0 Alt-Svc: quic=":443"; ma=2592000; v="44,43,39,35" Connection: close https://xxx.com/prod/register_hub HTTP/1.1 200 OK Content-Type: application/json Content-Length: 23 Connection: close Date: Fri, 13 Jul 2018 02:18:35 GMT x-amzn-RequestId: [redacted] x-amz-apigw-id: [redacted] X-Amzn-Trace-Id: [redacted];Sampled=0 X-Cache: Miss from cloudfront Via: 1.1 [redacted].net (CloudFront) X-Amz-Cf-Id: [redacted]			
2.4.13.3	All products related web servers have their webserver HTTP trace and trace methods disabled.	1 and above	M	TBD in future release
	N/A: Cloud server testing was out of scope of this assessment			
2.4.13.4	All the products related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	1 and above	M	TBD in future release
	PASS: [redacted] Valid Certificate Issued by Amazon Valid from Wednesday, December 6, 2017 12:00:00 AM Valid to Thursday, December 6, 2018 12:00:00 PM Subject organization Unknown Serial number [redacted] A8 SHA-256 fingerprint			

				
2.4.13.5	The Product Manufacturer or Service Provider has a process to monitor the relevant security advisories to ensure all the product related web servers use protocols with no publicly known weaknesses.	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	1 and above	M	TBD in future release

	PASS:
	Only secure negotiation supported
	`TLS renegotiation:`
	`Secure session renegotiation supported`
	`TLS renegotiation:`
	`Secure session renegotiation supported`			

2.4.13.8	The related servers have unused IP ports disabled.	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.11	All the related servers and network elements prevent the use of null or blank passwords	1 and above	M	TBD in future release
2.4.13.12	The Cloud and Network elements follow the password requirements of section 2.4.8.	1 and above	A	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.13	All the related servers and network elements prevent new passwords from containing the user account name, with which the user account is associated.	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.14	All the related servers and network elements enforce passwords to include: at least eight characters in length; characters from the groupings: alpha, numeric, and special characters and shall not	1 and above	M	TBD in future release

	be vulnerable to dictionary attack.			
	N/A: Out of scope of this engagement.			
2.4.13.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms, for example see FIPS 140-2 [ref 5].	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.18	All the related and network elements servers prevent anonymous/guest access except for read only access to public information.	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			
2.4.13.22	Input data validation should be maintained in accordance with industry practiced methods as per NIST SP 800-53 SI-10 [Ref 33].	1 and above	M	TBD in future release
	N/A: Out of scope of this engagement.			

Ownership Transfer Audit

This section's intended audience is for those personnel who are responsible for Data Protection and Device Ownership management.

The device did not support ownership transfer and is out of scope of this assessment.

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.16.1	Where a device or devices are capable of having their ownership transferred to a different owner, all the previous owners Personal Information shall be removed from the device(s) and registered services. This option must be available when a transfer of ownership occurs or when an end user wishes to delete their Personal Information from the service or device.	1 and above	M	TBD in future release
2.4.16.2	Where a device or devices user wishes to end the service, all that owners Personal Information shall be removed from the device and related services.	1 and above	M	TBD in future release
2.4.16.3	The Service Provider should not have the ability to do a reverse lookup of device ownership from the device identity.	2 and above	M	TBD in future release
2.4.16.4	In case of ownership change, the device has an irrevocable method of decommissioning and recommissioning.	1 and above	M	TBD in future release
2.4.16.5	The device registration with the Service Provider shall be secure (method and reasoning needed in evidence).	1 and above	M	TBD in future release
2.4.16.6	The device manufacturer ensures that the identity of the device is independent of the end user, to ensure anonymity and comply with relevant local data privacy laws e.g. GDPR in the EU.	1 and above	M	TBD in future release

7) Firmware, software and applications - Analysing binaries

Disassembly and emulation of firmware binaries, running the binaries so we can analyse/exploit them.

Tool Name	Description
Apktool	A tool for reversing Android apk files
Binwalk	A tool used for extracting filesystems from files
Firmadyne	Firmware analysis tool
gdb	GNU Debugger
IDA Pro	Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger
Immunity Debugger	A debugger similar to OllyDbg that has some cool plugins with the use of Python
OllyDbg	The most disassembly-based and GUI debugger for Windows
PE Tool	Provide a handful of useful tools for working with Windows PE executables
PEID	Used to determine if any obfuscator was used to pack the executable file. The open source packer that is often used is the UPX packer
Plasma	An Interactive Disassembler for x86/ARM/MIPS
QEMU	A tool for emulating different CPU architectures ARM/MIPS/PowerPC – use readelf -h file.bin to determine the firmware type
Radare2	Unix-like reverse engineering framework and command line tools
Shellphish	Static Code Analysis Tool
Strace	A system call tracer and another debugging tool
WinDbg	Windows Debugger distributed by Microsoft.

8) Firmware, software and applications - Exploiting binaries

Looking for security vulnerabilities within the binaries/setting breakpoints and creating exploits.

Tool Name	Description
Firmwalker	A tool which performs a static analysis on the firmware – extracting potentially interesting information.
Firmware Mod Kit	A tool which allows a firmware image to be extracted, add your own code, and build a new version of the firmware.

9) Manufacturer compliance/Audit sections

This section deals with manufacturer compliance and needs to be part of a manufacturer audit.
The following section is part of a supplier audit and is out of scope of this assessment.

Req. No	Requirement	Compliance Class	Category Applicability	
			A - Consumer	B - Enterprise
2.4.3.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	1 and above	M	TBD in future release
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	1 and above	M	TBD in future release
2.4.3.3	There are documented business processes in place for security.	1 and above	M	TBD in future release
2.4.3.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework ISO27000 series etc).	2 and above	A	TBD in future release
2.4.3.5	A policy has been established for dealing with both internal and third-party security researcher(s) on the products or services.	1 and above	M	TBD in future release
2.4.3.6	A security policy has been established for addressing changes, such as vulnerabilities, that could impact security and affect or involve technology or components incorporated into the product or service provided.	2 and above	A	TBD in future release
2.4.3.7	Processes and plans are in place based upon the IoTSF "Vulnerability Disclosure Guidelines" or a similar recognised process to deal with the identification of a security vulnerability or compromise when they occur.	1 and above	M	TBD in future release
2.4.3.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements. In particular, that any public statements made in the event of a security breach should give as full and accurate an account of the facts as possible.	1 and above	M	TBD in future release
2.4.3.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure	1 and above	M	TBD in future

	Guidelines" or similar recognised process, for notifying partners/users of any security updates.			release
2.4.3.10	A security threat and risk assessment shall have been carried out using a standard methodology such as Octave or NIST SP 800-37 Rev. 1 Risk Management Framework [ref 35] to determine the risks and evolving threats.	2 and above	A	TBD in future release
2.4.3.11	As part of the Security Policy develop specific contact web pages for Vulnerability Disclosure reporting.	1 and above	M	TBD in future release
2.4.3.12	As part of the Security Policy, provide a dedicated security email address and/or secure webform for Vulnerability Disclosure communications.	1 and above	M	TBD in future release
2.4.3.13	As part of the Security Policy publish the organisation's conflict resolution process for Vulnerability Disclosures.	1 and above	A	TBD in future release
2.4.3.14	As part of the Security Policy develop response steps and performance targets for Vulnerability Disclosures.	1 and above	M	TBD in future release
2.4.3.15	As part of the Security Policy develop security advisory notification steps.	1 and above	M	TBD in future release
2.4.3.16	The Security Policy shall be compliant with ISO30111 or similar standard.	1 and above	A	TBD in future release
2.4.3.17	Where real-time or up-time expectations are present, a mechanism must be present for notifying connected components of impending downtime for updates.	1 and above	A	TBD in future release
2.4.3.18	Responsibility is allocated for each stage of the update/updating lifecycle.	2 and above	A	TBD in future release
2.4.3.19	Responsibility is allocated for control of the update process.	2 and above	A	TBD in future release
2.4.3.20	Responsibility is allocated for logging and auditing the update process.	2 and above	A	TBD in future release
2.4.3.21	There is a point of contact for third party suppliers with update issues.	1 and above	A	TBD in future release
2.4.3.22	Where remote update is supported, there is an established process/plan for validating and updating updates on an on-going or remedial basis.	2 and above	A	TBD in future release

2.4.3.23	The security update policy for devices with a constrained power source shall be assessed to balance the needs of maintaining the integrity and availability of the device.	2 and above	A	TBD in future release
2.4.3.24	There is a named owner responsible for assessing third party supplied components (hardware and software) used in the product e.g. have the OS suppliers provided a completed "IoTSF Framework" document or equivalent.	1 and above	A	TBD in future release
2.4.3.25	Where remote software upgrade can be supported by the device, there should be a published/transparent and auditable policy and schedule of actions to fix any vulnerabilities found.	1 and above	A	TBD in future release

2.4.5 Compliance Applicability - Device Software
This section's intended audience is for those personnel who are responsible for device application quality.

Compliance Applicability – Secure Supply Chain and Production This section's intended audience is for those personnel who are responsible for the security of the IoT Product or Services' Supply Chain.

2.4.5.15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example, security related processes should be executed at higher privilege levels in the application processor hardware	1 and above	M	
2.4.5.16	Software source code is developed, tested and maintained following defined repeatable processes.	2 and above	A	TBD in future release
2.4.5.17	The build environment and toolchain used to compile the application is run on a build system with controlled and auditable access.	2 and above	A	TBD in future release
2.4.5.18	The build environment and toolchain used to create the software is under configuration management and version control, and its integrity is validated regularly.	2 and above	A	TBD in future release
2.4.5.19	The production software signing keys are under access control.	1 and above	M	TBD in future release
2.4.5.20	The production software signing keys are stored and secured in a storage device compliant to FIPS-140 level 2, or equivalent or higher standard.	2 and above	A	TBD in future release
2.4.14.1	The product has all of the production test and calibration software used during manufacture erased or removed or secured before the product is dispatched from the factory. This is to prevent alteration of the product post manufacture when using authorised production software, for example hacking of the RF characteristics for greater RF ERP. Where such functionality is required in a service centre, it shall be erased or removed upon completion of any servicing activities.	2 and above	A	TBD in future release
2.4.14.2	In manufacture, all encryption keys that are unique to each device are either securely and truly randomly internally generated or securely programmed into each device in accordance with industry standard FIPS 140-2 [ref 5] or equivalent. Any secret key programmed into a product at manufacture is unique to that individual device, i.e. no global secret key is shared between multiple devices. – unless this is required by a licensing authority.	2 and above	A	TBD in future release
2.4.14.3	In manufacture, all the devices are logged by the product vendor, so that cloned or duplicated devices can be identified and either disabled or prevented from being	1 and above	M	TBD in future release

	used with the system.			
2.4.14.4	The production system for a device has a process to ensure that any devices with duplicate serial numbers are not shipped and are either reprogrammed or destroyed.	1 and above	M	TBD in future release
2.4.14.5	Where a product includes a trusted Secure Boot process, the entire production test and any related calibration is executed with the processor system operating in its secured boot, authenticated software mode.	2 and above	A	TBD in future release
2.4.14.6	A securely controlled area and process shall be used for device provisioning where the production facility is untrusted. For example, implement the controls required in Common Criteria EAL5+/6 certification.	2 and above	A	TBD in future release

2.4.15 Compliance Applicability – Configuration

This section's intended audience is for those personnel who are responsible for the security of the device and IoT Services configurations.

2.4.15.1	The configuration of the device and any related web services is tampering resistant. i.e. sensitive configuration parameters should only be changeable by authorised people (evidence should list the parameters and who is authorised to change).	1 and above	M	TBD in future release

Appendix A – Severity Scale

Vulnerabilities are supplied with corresponding ratings indicating their severity, and these are rated on a scale of one to five using the icons below.

A rating of five means that the vulnerability could enable an attacker to compromise the device, and a rating of one is of low severity.

A more detailed description of the rating system, including examples, can be found in the table below:

Severity	Description
●○○○○ INFO (CVSS 0)	Level 1 issues are raised purely for **informational** purposes and do not pose any risks to security. The reason for their inclusion is to make the customer aware of their presence in case their status was to change. For example, sensitive entries in a robots.txt file may not be accessible at the time of testing, but may become accessible in the future.
●●○○○ LOW (CVSS 0.1-3.9)	Level 2 vulnerabilities pose a **low** threat to security. Low threat issues include for example: Leakage of information (such as software versions) which an attacker may find useful; exposure of unnecessary content/functionality; configurations that do not meet best security practice.
●●●○○ MEDIUM (CVSS 4-6.9)	Level 3 vulnerabilities pose a **medium** threat to security. Medium-risk issues could allow an attacker to gain limited access to system commands or sensitive data. In addition, vulnerabilities addressed as medium risk when combined with other factors could have a high impact on security if exploited.
●●●●○ HIGH (CVSS 7-9.9)	Level 4 vulnerabilities pose a **high** threat to security. Issues are raised as high-threat when exploitation could result in a major security breach, such as allowing attackers to gain privileged access, escalate privileges, or to access/modify/remove sensitive information and/or functionality.
●●●●● CRITICAL (CVSS 10)	Level 5 vulnerabilities pose a **critical** threat to security. Security issues raised at this level would generally allow an attacker to gain unauthorised access to a system or sensitive data using publicly-available tools and exploits. As an example, if a host was found to be running an unsupported operating system for which exploits were publicly available, this would qualify as a level 5. If fully exploited such vulnerabilities could have disastrous effects on the business.