internet of secure things

COMPANY

DEVICE

SKU

Firmware Version

Quarterly Compliance Report

Q3 2020

Contents

1.0 INTRODUCTION 4

- 1.1 Reporting Period 4
- 1.2 Disclaimer 4

2.0 EXECUTIVE SUMMARY 6

- 2.1 Product Certification Summary 6
  - 2.1.1 Certification Details 6
  - 2.1.2 Certification Disputes Under Review 7
- 2.2 Security Alerts Summary 7
- 2.3 Regulatory Review Summary 8
  - 2.3.1 NIST 9
  - 2.3.2 ETSI 9
- 2.4 Compliance Test Report Summary 10

3.0 DEVICE CERTIFICATION 12

- 3.1 Summary 12
- 3.2 New and Pending Certification Disputes 13
- 3.3 Disputes and Rewards Reports 13
  - 3.3.1 Reporting Period Disputes and Rewards 14
  - 3.3.2 Lifetime Disputes and Rewards 14

4.0 SECURITY ALERTS 16

- 4.1 Summary 16
- 4.2 New Security Alerts 16
- 4.3 Lifetime Security Alerts 20
- 4.4 Security Alert News 22
- 4.5 Dark Web Security Alerts 24

5.0 REGULATORY REVIEW 25

- 5.1 Summary 25
- 5.2 NIST Review 26
- 5.3 ETSI Review 29
- 5.4 ISO Review 35
- 5.5 IEC Review 35
- 5.6 Regulatory News 36

6.0 COMPLIANCE TEST REPORT 38

6.1 VDP – Vulnerability Reporting Program 38
6.2 SE – Security Expiration 38
6.3 AA – Automatically Applied Updates 38
6.4 VS – Verified Software 39
6.5 PC – Proven Cryptography 39
6.6 SI – Secured Interfaces 40
    6.6.1 Ethernet 40
    6.6.2 Wi-Fi 40
    6.6.3 Zigbee 41
6.7 SD – Security by Default 41
6.8 UP – No Universal Password 42

1.0 INTRODUCTION

This Quarterly Compliance Report profiles the **COMPANY DEVICE**, certified by the ioXt Alliance (the "Alliance") through its security certification program (the "Certification Program"). Learn more about the Alliance and the Certification Program **here**, or for a closer look, view the DEVICE's dedicated **product page**. A mobile version of the product page is also available via the SmartCert logo included in Section 2.1.

The purpose of this compliance report is to provide you, the registered manufacturer, an outline of your device's security certification, updates to the device's ongoing compliance, and alerts for possible threats to the device and its ecosystem.

The following sections will walk you through an Executive Summary (Section 2.0), the Device Certification status (3.0), new and lifetime Security Alerts (4.0), a Regulatory Review (5.0), and the latest device Compliance Test Report (6.0). Also, as new alerts arise, the Alliance will provide real-time updates and notifications via email and your **portal dashboard**.

Recent additions to the report include sections 4.4 and 5.6, which contain the Alliance's latest digest of news, trends, and developments from around the IoT world.

Please submit any questions or comments to **security@ioxt.com** or within the Alliance **Member Portal**, which is available to all Certification Program participants. Thank you for joining the **ioXt Alliance**, the Global Standard for IoT Security.

1.1 Reporting Period

The reporting period for this compliance report is July 8, 2020 – August 31, 2020 (the "Reporting Period").

Any "new" activity in the report is for the Reporting Period. Total or "lifetime" activity includes all alerts, updates, and information from the device's first quarterly compliance report through the end date of the Reporting Period.

No data is captured beyond the end date of the Reporting Period.

1.2 Disclaimer

The Alliance presents this report for informational purposes only, without any warranty of any kind, and in accordance with the Subscription and Certification Services Agreement (the "Agreement") and the Product Subscription Addendum (the "Addendum") between you and the Alliance.

Both the Agreement and the Addendum can be found in the documents section of your **portal dashboard** referenced above.

THE IOXT ALLIANCE DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD-PARTIES, OR ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR USE, TITLE, NON-INFRINGEMENT, OR GUARANTEE OF PRODUCT SECURITY. IN NO EVENT WILL THE IOXT ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN.

2.0 EXECUTIVE SUMMARY

This section is an executive summary of the DEVICE compliance report. More details about the device's certification, security alerts, and regulatory mapping are found in the subsequent sections.

2.1 Product Certification Summary

The DEVICE was initially certified on July 8, 2020 and has maintained its certification throughout the Reporting Period. View your device's certification status and specifications **here**. As a certified device, the DEVICE also has a unique, live SmartCert logo to direct channel owners, retailers, and end users to its ioXt mobile certification page:

Within the mobile page, consumers can see a device's CERTIFIED stamp, product specs, and levels of compliance. Remember, the SmartCert logo has replaced the original ioXt check mark and may be placed on a device's packaging or even the device itself. It serves as the gateway into the certification status and specifications for the lifetime of your product.

2.1.1 Certification Details

Here are the certification details, including firmware version, for the DEVICE:

Product:	DEVICE
SKU:	SKU
Firmware Version:	Firmware Version
Certification Date:	7/8/2020
Certification Number:	2020070004
Certification Profile:	ioXt 2020 Base
Certification Method:	Manufacturer Certified

Test Lab: N/A

The DEVICE was certified against the ioXt 2020 Base profile. View the profile or learn more about the profile test cases **here**. The latest Test Case Library has also been uploaded to the documents section of your **portal dashboard**.

2.1.2 Certification Disputes Under Review

Independent researchers play a vital role in validating each certified device's continued compliance with the **ioXt Security Pledge**. These researches may submit disputes against devices for pledge levels in question. For any dispute validated by the Alliance, researchers receive monetary rewards, or bounties.

Here are the disputes for the DEVICE currently under Alliance review. All lifetime rewards paid out against the DEVICE are outlined in Section 3.3.2:

DISPUTES UNDER REVIEW – DEVICE

Pledge	Test Case	Dispute Summary	Dispute ID	Dispute Date

Table 2.1.2 *Certification Disputes Currently Under Review*

Congratulations, the DEVICE has no disputes under review

The Alliance reviews all disputes, and if valid, presents them to you for resolution. Find out more about the dispute process and ioXt's Researcher Rewards program **here**.

2.2 Security Alerts Summary

This is a summary of the security alert activities for the DEVICE during the Reporting Period. More details regarding the nature and severity levels of the alerts can be found in Section 4.0.

There are **19** new security alerts for the DEVICE, bringing the its lifetime total to **19**.

Security Alerts – DEVICE

19	19
New Security Alerts	Lifetime Security Alerts

Alerts are warnings of possible security issues, but do not necessarily imply a serious threat or vulnerability. The LIKELIHOOD level is a guide for the relevance of each identified vulnerability to your device. While not affecting your device's certification status, these alerts may serve as an indicator for future certification disputes.

The following table is a heat map of new security alerts for the DEVICE:

NEW ALERT HEAT MAP – DEVICE

NEW ALERT SUMMARY **Q3 2020**		SEVERITY			
		CRITICAL	**HIGH**	**MEDIUM**	**LOW**
LIKELIHOOD	**HIGH**	-	3	-	-
	MEDIUM	-	1	-	-
	LOW	8	5	2	-

Table 2.2.1 *Heat Map of New Alerts, Q3 2020*

In Table 2.2.1, LIKELIHOOD refers to the applicability of the vulnerability to your device and SEVERITY refers to a qualitative ranking provided by the National Institute of Standards and Technology (NIST) within its National Vulnerability Database (NVD). Learn more about the NVD and its vulnerabilities metrics **here**.

See Section 4.2 for more details on the heat map alerts. A full vulnerability, also known as a **CVE**, description is included for any alert labeled HIGH (or CRITICAL) in severity as well as HIGH in likelihood.

2.3 Regulatory Review Summary

An important benefit of your Alliance certification and subscription is a review of your device's alignment with other IoT regulatory standards. This report focuses on the two preeminent bodies for IoT regulation, NIST in the United States and the European Telecommunications Standards Institute (ETSI) in Europe and around the world.

While not an exhaustive or conclusive mapping, Section 5.0 outlines your device against the applicable NIST and ETSI IoT standards.

2.3.1 NIST

NIST, an organization within the U.S. Commerce Department, has developed security standards specifically for IoT connected devices. Based on the information provided in the ioXt Certification Portal, the DEVICE has been evaluated to pass, or partially pass, **48%** of the NIST standards:

NIST REGULATORY MAPPING – DEVICE

8	3	12	0
Pass Evaluations	Partial Evaluations	Unknown Evaluations	Fail Evaluations

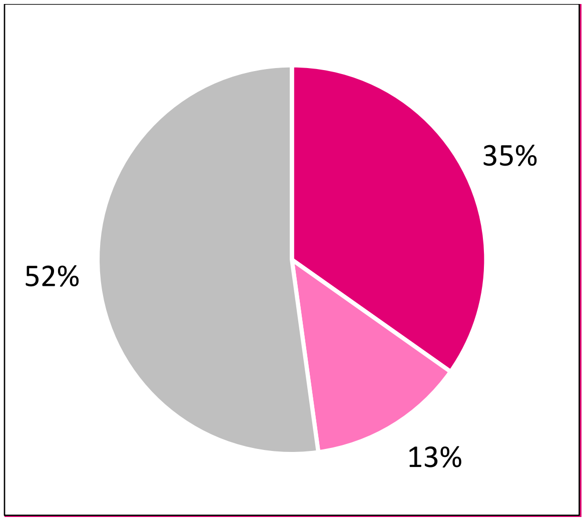


Figure 2.3.1 *NIST Regulatory Mapping*

Section 5.2 provides more details of the NIST publications and the specific NIST provisions met by the DEVICE.

2.3.2 ETSI

ETSI, a not-for-profit standards organization based in Europe, has developed its own, consumer-driven security standards for IoT devices. Based on the information provided in the ioXt Certification Portal, the DEVICE has been evaluated to pass, or partially pass, **41%** of the ETSI standards:

ETSI REGULATORY MAPPING – DEVICE

26	0	27	10
Pass Evaluations	Partial Evaluations	Unknown Evaluations	Fail Evaluations

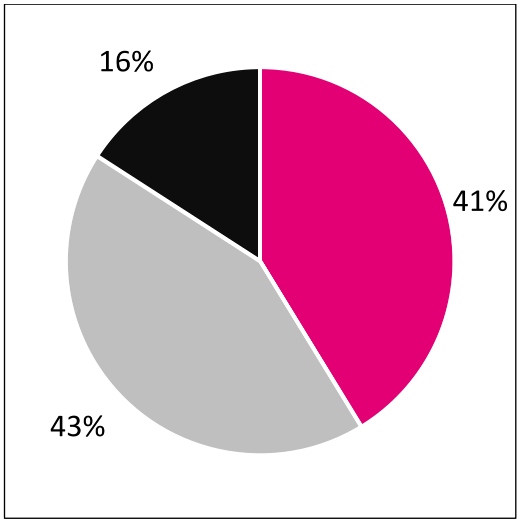


Figure 2.3.2 *ETSI Regulatory Mapping*

Section 5.3 provides more details of the ETSI publications and the specific ETSI provisions met by the DEVICE.

2.4 Compliance Test Report Summary

The **ioXt Security Pledge** brings security, upgradability, and transparency to the IoT marketplace through its eight core principals. To pass certification a device must meet the minimum pledge levels described in the Alliance Pledge Booklet.

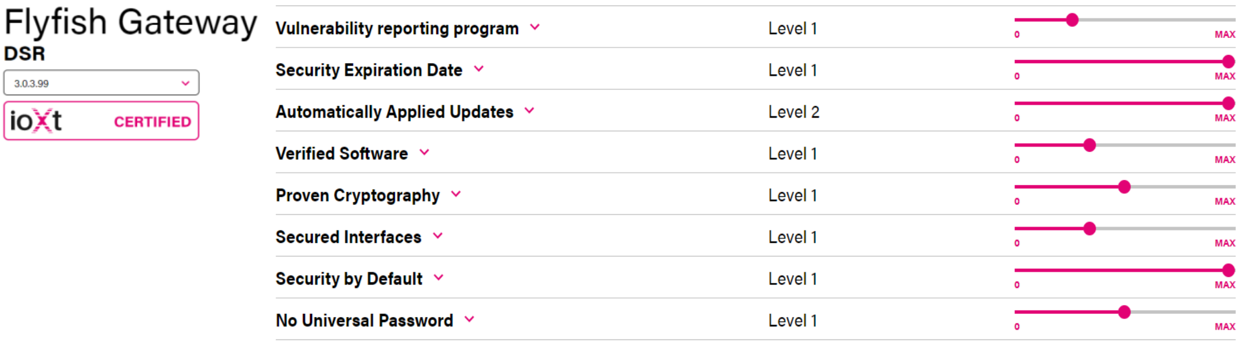
The DEVICE has achieved certification for the ioXt 2020 Base profile at the levels set forth below. Section 3.0 provides further detail on its certification status and Section 6.0 contains the full compliance report:

PLEDGE LEVELS – DEVICE

Pledge	Level Achieved
P1 – Vulnerability Reporting Program	1
P2 – Security Expiration Date	1
P3 – Automatically Applied Updates	2

P4 – Verified Software	1
P5 – Proven Cryptography	1
P6 – Secured Interfaces	1
P7 – Security by Default	1
P8 – No Universal Password	1

Table 2.4.1 *Compliance Pledge Levels*



Flyfish Gateway

DSR

3.0.3.99

ioXt CERTIFIED

Vulnerability reporting program	Level 1
Security Expiration Date	Level 1
Automatically Applied Updates	Level 2
Verified Software	Level 1
Proven Cryptography	Level 1
Secured Interfaces	Level 1
Security by Default	Level 1
No Universal Password	Level 1

Table 2.4.2 *Compliance Pledge Levels – Product Page*

Learn more about the pledges and download the ioXt Pledge Booklet **here**.

3.0 DEVICE CERTIFICATION

This section outlines the DEVICE's certification status along with a dispute and researcher rewards breakdown. To view its real-time status, visit the DEVICE's **product page** or follow the SmartCert logo above.

3.1 Summary

The DEVICE achieved certification for the ioXt 2020 Base profile on July 8, 2020 and has maintained its certification throughout the Reporting Period.

Independent researchers have submitted a total of **0** new disputes against the DEVICE, **0** of which have been validated by the Alliance for **$0.⁰⁰** of new rewards paid. During its lifetime, there have been a total of **0** disputes submitted, **0** of which have been validated by the Alliance for **$0.⁰⁰** of total rewards paid.

Here are the current certification levels for the DEVICE:

DEVICE – ioXt 2020 BASE PROFILE

Pledge	Device Level	Certification Min Level	Profile Max Level	Next Level Test Cases
P1 – Vulnerability Reporting Program	1	1	4	VDP3, VDP4, VDP5
P2 – Security Expiration Date	1	1	1	MAX
P3 – Automatically Applied Updates	2	1	2	MAX
P4 – Verified Software	1	1	3	VS5, VS6
P5 – Proven Cryptography	1	1	2	PC2
P6 – Secured Interfaces	1	1	3	SI2, SI3
P7 – Security by Default	1	1	1	MAX
P8 – No Universal Password	1	1	2	UP2

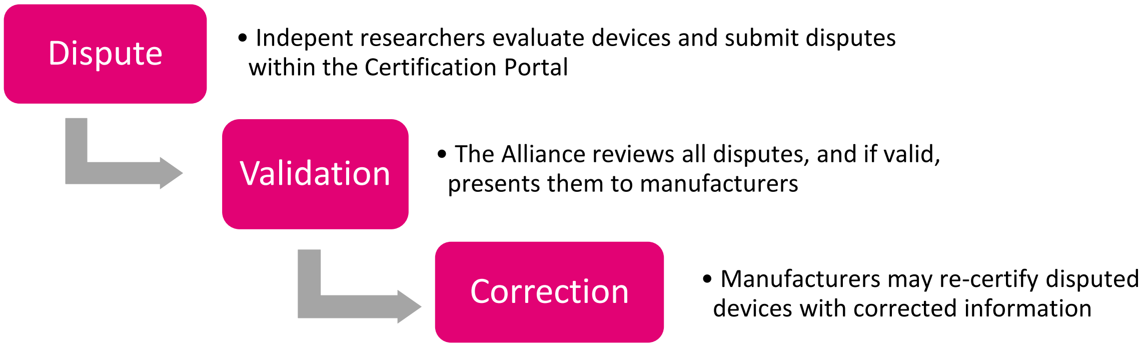
Table 3.1.1 *Certification Levels Against the Applicable Profile*

Table 3.1.1 shows how your device matches against the ioXt 2020 Base profile, the max level achievable under the profile, and importantly, which additional Next Level Test Cases are available. While not necessary to maintain certification, the next level cases indicate opportunities to make the DEVICE even more secure against threats and vulnerabilities.

Congratulations, the DEVICE has reached max certification levels for Security Expiration Date, Automatically Applied Updates, and Security by Default

3.2 New and Pending Certification Disputes

Throughout the lifetime of your device’s certification, independent researchers and affiliates can dispute the achieved pledge levels. To incentivize and facilitate a robust dialogue between manufacturers and researchers, the Alliance has created the **Researcher Rewards** program to validate and compensate any legitimate disputes.



Dispute

- Indepent researchers evaluate devices and submit disputes within the Certification Portal

Validation

- The Alliance reviews all disputes, and if valid, presents them to manufacturers

Correction

- Manufacturers may re-certify disputed devices with corrected information

View the dispute schedule and tiers of rewards **here**. The following are the new and pending disputes for the DEVICE:

NEW AND PENDING DISPUTE REPORT – DEVICE

Pledge	Test Case	Dispute Summary	Dispute ID	Dispute Date	Status

Table 3.2.1 New and Pending Dispute Summary

Congratulations, the DEVICE has no new or pending disputes

Click on the Dispute IDs above for more details or visit your **portal dashboard** to view and address all pending disputes. The Alliance will continuously monitor new submissions against your device and will provide dispute notifications via email and within the Certification Portal.

3.3 Disputes and Rewards Reports

As highlighted above, independent researchers may receive monetary rewards for validated disputes. Section 3.3.1 and Section 3.3.2 contain the dispute rewards received for the Reporting Period and lifetime of the DEVICE, respectively.

3.3.1 Reporting Period Disputes and Rewards

New disputes submitted against the DEVICE during the Reporting Period:

NEW DISPUTE PIPELINE – DEVICE

New Disputes Submitted	Pending ioXt Review	Pending COMPANY Review	COMPANY Accepted-Corrected	COMPANY Rejected	Escalated to Board
0	0	0	0	0	0

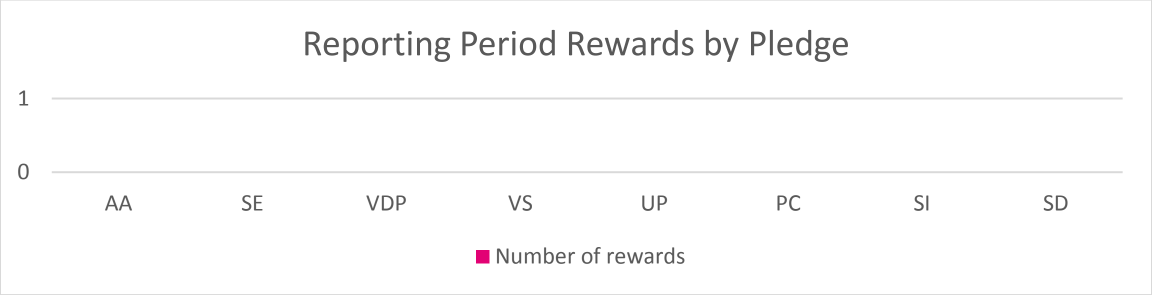


Figure 3.3.1 *Reporting Period Rewards Paid by Pledge*

3.3.2 Lifetime Disputes and Rewards

Total disputes submitted against the DEVICE during its lifetime:

LIFETIME DISPUTE PIPELINE – DEVICE

Total Disputes Submitted	Pending ioXt Review	Pending COMPANY Review	COMPANY Accepted-Corrected	COMPANY Rejected	Escalated to Board
0	0	0	0	0	0

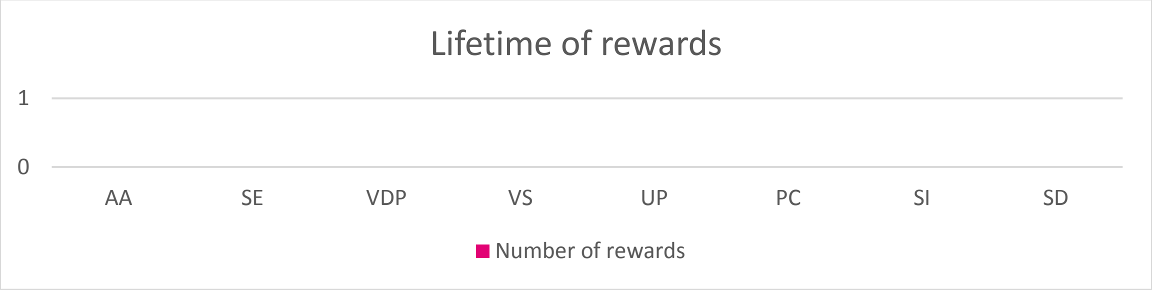


Figure 3.3.2 *Lifetime Rewards Paid by Pledge*

4.0 SECURITY ALERTS

This section highlights potential security issues relating to the DEVICE by matching the device specifications to publicly known vulnerabilities and exposures within NIST's NVD database.

Security alerts are threats and vulnerabilities from the NVD database that have the potential to affect specific hardware and software within your device. If a device has a security alert, it does not mean that the product is necessarily insecure, just that there is a potential threat or vulnerability for review.

4.1 Summary

The NVD database contains Common Vulnerabilities and Exposures (CVE) entries, a dictionary of publicly disclosed cybersecurity vulnerabilities and exposures.

Use of CVE entries, which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provides a baseline tool for evaluation, and enables automated data exchange.

In short, a **CVE** is**:**

- An identifier for one vulnerability or exposure
- A standardized description for each vulnerability or exposure
- A basis for evaluation among services, tools, and databases

Security Alerts – DEVICE

19	19
New Security Alerts	Lifetime Security Alerts

Section 4.2 and Section 4.3 provide more detail of the alerts identified for the DEVICE over the Reporting Period and its lifetime. Pay particular attention to the HIGH alerts, which are most applicable to your device and include a detailed vulnerability description.

4.2 New Security Alerts

There are **19** new security alerts for the DEVICE.

Tables 4.2.1 – 4.2.5 list in detail which vulnerabilities were identified as alerts. To trigger a new security alert, the vulnerability must have been newly added to the CVE database during the Reporting Period.

In the heat map table, 'LIKELIHOOD' refers to applicability of the vulnerability to your specific device and 'SEVERITY' refers to a qualitative severity ranking provided by NIST through its National Vulnerability Database (NVD). Learn more about the NVD and its vulnerabilities metrics **here**:

NEW ALERT HEAT MAP – DEVICE

NEW ALERT SUMMARY **Q3 2020**		SEVERITY			
		CRITICAL	**HIGH**	**MEDIUM**	**LOW**
LIKELIHOOD	**HIGH**	-	3	-	-
	MEDIUM	-	1	-	-
	LOW	8	5	2	-

Table 4.2.1 *Heat Map of New Alerts, Q3 2020*

Tables 4.2.2 – 4.2.5 divide the new security alerts by 'Likelihood' score – HIGH, MEDIUM, and LOW. The score measures the severity and applicability of each vulnerability to your product using the components and categories outlined in the tables.

'Component' refers to the software, hardware, or security libraries used to search the NVD database, and 'Category' refers to how the value matches a CPE related to the particular CVE entry.

HIGH LIKELIHOOD ALERTS	CVE's where a related CPE directly matches the component at the product level
MEDIUM LIKELIHOOD ALERTS	CVE's where a related CPE directly matches the component vendor, but for a different product
LOW LIKELIHOOD ALERTS	CVEs where the CVE description contains a component vendor/product match, but not the related CPE
LOW INTERFACE ALERTS	CVEs where a related CPE matches one or more of the product's interfaces

For the HIGH scores, further detail has been provided, including the CVE general description and the analysis description. More information can be found about each vulnerability by clicking the specific CVE

HIGH LIKELIHOOD ALERTS – DEVICE

	CVE Identifier	Severity Score	Likelihood Score	Category	Component	Date
1	CVE-2019-19945	HIGH – 7.5	HIGH	Product	OpenWRT	3/16/2020
2	CVE-2020-1967	HIGH – 7.5	HIGH	Product	OpenSSL	4/21/2020
3	CVE-2020-7248	HIGH – 7.5	HIGH	Product	OpenWRT	3/16/2020
	TOTAL VULNERABILITIES = 3					

Table 4.2.2 *New Security Alerts – High Likelihood of Product Impact*

CVE-2019-19945 (High – 7.5)

Current Description
“uhttpd in OpenWrt through 18.06.5 and 19.x through 19.07.0-rc2 has an integer signedness error. This leads to out-of-bounds access to a heap buffer and a subsequent crash. It can be triggered with an HTTP POST request to a CGI script, specifying both "Transfer-Encoding: chunked" and a large negative Content-Length value.”

Analysis Description
“uhttpd in OpenWrt through 18.06.5 and 19.x through 19.07.0-rc2 has an integer signedness error. This leads to out-of-bounds access to a heap buffer and a subsequent crash. It can be triggered with an HTTP POST request to a CGI script, specifying both "Transfer-Encoding: chunked" and a large negative Content-Length value.”

CVE-2020-1967 (HIGH – 7.5)

Current Description
“Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).

Analysis Description
“Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).”

CVE-2020-7248 (HIGH – 7.5)

Current Description
"libubox in OpenWrt before 18.06.7 and 19.x before 19.07.1 has a tagged binary data JSON serialization vulnerability that may cause a stack based buffer overflow."

Analysis Description
"libubox in OpenWrt before 18.06.7 and 19.x before 19.07.1 has a tagged binary data JSON serialization vulnerability that may cause a stack based buffer overflow."

MEDIUM LIKELIHOOD ALERTS – DEVICE

	CVE Identifier	Severity Score	Likelihood Score	Category	Component	Date
1	CVE-2020-7982	HIGH – 8.0	MEDIUM	Vendor	OpenWRT	3/16/2020
TOTAL VULNERABILITIES = 1						

Table 4.2.3 *New Security Alerts – Medium Likelihood of Product Impact*

LOW LIKELIHOOD ALERTS – DEVICE

	CVE Identifier	Severity Score	Likelihood Score	Category	Component	Date
1	CVE-2019-14887	CRITICAL – 9.0	LOW	Indirect	OpenSSL	3/16/2020
2	CVE-2019-17185	HIGH – 7.5	LOW	Indirect	OpenSSL	3/20/2020
3	CVE-2020-7041	MEDIUM – 5.0	LOW	Indirect	OpenSSL	2/27/2020
4	CVE-2020-7042	MEDIUM – 5.0	LOW	Indirect	OpenSSL	2/27/2020
5	CVE-2020-7043	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/220
6	CVE-2020-7224	CRITICAL – 9.5	LOW	Indirect	OpenSSL	4/16/2020
7	CVE-2020-9432	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/2020
8	CVE-2020-9433	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/2020
9	CVE-2020-9434	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/2020
10	CVE-2020-13417	CRITICAL – 9.5	LOW	Indirect	OpenSSL	5/22/2020
11	CVE-2020-13962	HIGH – 7.5	LOW	Indirect	OpenSSL	6/8/2020
12	CVE-2020-14396	HIGH – 7.5	LOW	Indirect	OpenSSL	6/17/2020
TOTAL VULNERABILITIES = 12						

Table 4.2.4 *New Security Alerts – Low Likelihood of Product Impact*

LOW INTERFACE ALERTS – DEVICE

	CVE Identifier	Severity Score	Likelihood Score	Category	Component	Date
1	CVE-2019-20480	HIGH – 8.5	LOW	Interface	Zigbee	2/24/2020
2	CVE-2019-20481	CRITICAL – 9.5	LOW	Interface	Zigbee	2/24/2020
3	CVE-2020-7476	HIGH – 7.5	LOW	Interface	Zigbee	3/23/2020
TOTAL VULNERABILITIES = 3						

Table 4.2.5 *New Security Alerts – Applicable Interfaces*

4.3 Lifetime Security Alerts

There are **19** lifetime security alerts for the DEVICE.

Table 4.3.1 serves as a running reference list of CVE entries flagged for the DEVICE throughout its lifetime of compliance reports:

LIFETIME OF SECURITY ALERTS – DEVICE

	CVE Identifier	Severity Score	Likelihood Score	Category	Flag Value	Published Date
1	CVE-2019-19945	HIGH – 7.5	HIGH	Product	OpenWRT	3/16/2020
2	CVE-2020-1967	HIGH – 7.5	HIGH	Product	OpenSSL	4/21/2020
3	CVE-2020-7248	HIGH – 7.5	HIGH	Product	OpenWRT	3/16/2020
4	CVE-2020-7982	HIGH – 8.0	MEDIUM	Vendor	OpenWRT	3/16/2020
5	CVE-2019-14887	CRITICAL – 9.0	LOW	Indirect	OpenSSL	3/16/2020
6	CVE-2019-17185	HIGH – 7.5	LOW	Indirect	OpenSSL	3/20/2020
7	CVE-2020-7041	MEDIUM – 5.0	LOW	Indirect	OpenSSL	2/27/2020
8	CVE-2020-7042	MEDIUM – 5.0	LOW	Indirect	OpenSSL	2/27/2020
9	CVE-2020-7043	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/220
10	CVE-2020-7224	CRITICAL – 9.5	LOW	Indirect	OpenSSL	4/16/2020

11	**CVE-2020-9432**	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/2020
12	**CVE-2020-9433**	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/2020
13	**CVE-2020-9434**	CRITICAL – 9.0	LOW	Indirect	OpenSSL	2/27/2020
14	**CVE-2020-13417**	CRITICAL – 9.5	LOW	Indirect	OpenSSL	5/22/2020
15	**CVE-2020-13962**	HIGH – 7.5	LOW	Indirect	OpenSSL	6/8/2020
16	**CVE-2020-14396**	HIGH – 7.5	LOW	Indirect	OpenSSL	6/17/2020
17	**CVE-2019-20480**	HIGH – 8.5	LOW	Interface	Zigbee	2/24/2020
18	**CVE-2019-20481**	CRITICAL – 9.5	LOW	Interface	Zigbee	2/24/2020
19	**CVE-2020-7476**	HIGH – 7.5	LOW	Interface	Zigbee	3/23/2020

Table 4.3.1 *Lifetime Security Alerts*

4.4 Security Alert News

What's new in IoT security? See below for the Alliance's latest digest of security news, trends, and developments in the world of IoT.

Smart-lock Hacks Point to Larger IoT Problems
Two recent reports on smart-locks vulnerabilities show that IoT vendors have a bigger job to do in ensuring their products are safely deployed and configured
DARKReading ▪ Aug 20

DARK
Reading
Get weekly updates on emerging security threats, vulnerabilities, and next-gen technology
Join Our Newsletter

Hackers are Exploiting the 'Internet of Things'
How to stay cyber secure? The answer lies in early detection and taking a holistic approach
ITProPortal ▪ Aug 25

The Internet of (Creepy Spy-ey) Things
I'm just stating the obvious. But I think it's worth re-stating because most of you are not cyber security researchers by day and may not remember the many reported examples of security and privacy violations over the years…
Forbes ▪ Sept 1

Researchers Discovered a New Vulnerability That Could Put Millions of IoT Devices at Risk
Patches have been issued for a vulnerability in a widely-used module in IoT devices, and researchers are urging IoT manufacturers to make sure that they applied the fixes. According to security researchers
Digital Information World ▪ Aug 22

SentinelOne Uncovers IoT Vulnerabilities Enabling Remote Takeover and Network Intrusion
SentinelOne, the autonomous cybersecurity platform company, has announced that Barak Sternberg, SentinelLabs security researcher, has identified four unique vulnerabilities…
Tahawultech.com ▪ Aug 11

Ripple20 Vulnerabilities Still Plaguing IoT Devices
Months after Ripple20 vulnerabilities were reported, things haven't gotten much better, say experts at Black Hat USA 2020. In fact…
Search Security ▪ Aug 6

Ready for IoT Security?
Big data will be collected from IoT devices. IoT device accuracy both in the data produced and its transmission must be near flawless

IoT Evolution ▪ Aug 18

Security in IoT – Why It Matters
IoT has quickly changed how we think of the Internet. Those who grew up with the Internet might still think of browsers on client systems like laptops and desktops
CPO Magazine ▪ Aug 6

In addition to the articles above, visit the News & Events section of the **Alliance website** to view all current ioXt happenings, including the latest press releases, events, blogs, newsletters, and much more!

4.5 Dark Web Security Alerts

COMING SOON

The Alliance is currently developing a new compliance report feature, which will include a summary of relevant IoT security alerts found across the darker reaches of the internet

5.0 REGULATORY REVIEW

This section outlines the global regulatory landscape for IoT security and evaluates your device's compliance against international regulatory bodies, primarily NIST, through its IoT device driven core baseline[1], and ETSI, though its consumer focused IoT baseline requirements.[2]

5.1 Summary

The regulatory review begins with the ioXt compliance evaluation and then maps to the outside standards. To account for the differences between the ioXt **pledge standards** and the various regulatory baselines, there are four evaluation grades for each regulatory element. Grades of PASS or PARTIAL indicate that your devices is likely to comply with the specific regulatory requirement:

Evaluation	**Description**	
PASS	The device is likely to comply with the regulatory requirement.	🟥
PARTIAL	The device is likely to comply at least somewhat with the regulatory requirement.	🟪
UNKNOWN	No meaningful evaluation is possible based on the ioXt yardstick, because the regulatory requirement does not have an ioXt pledge approximation.	▨
FAIL	The device is likely to not comply with the regulatory requirement.	⬛

This review serves as a helpful snapshot of where your device falls in the regulatory schemes and assists your organization in preparing the device to meet other standards. Note that this review is for informational purposes only and to help gauge your device's compliance with outside bodies.

---

[1] NISTIR 8259 A, Iot Device Cybersecurity Capability Core Baseline, Fagan, Megas, Scarfone, Smith, May 2020 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

[2] ETSI EN 303 645 V2.1.1, Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, June 2020 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

5.2 NIST Review

NIST, formerly the National Bureau of Standards, was founded in 1901 and now operates within the U.S. Department of Commerce. As one of the oldest physical science laboratories in the country, NIST has established technologies, measurement capabilities, and standards relied upon by countless devices and products in the IoT marketplace and beyond.

In May 2020, NIST released its Foundational Cybersecurity Activities for IoT Device Manufacturers (NISTIR 8259) along with the IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259 A). Together, NISTIR 8259 and NISTIR 8259 A established a federal profile for IoT devices with requirements ranging from the ability to restrict configuration changes to the ability to logically restrict access to network interfaces.

This section maps your device against the NIST baseline.

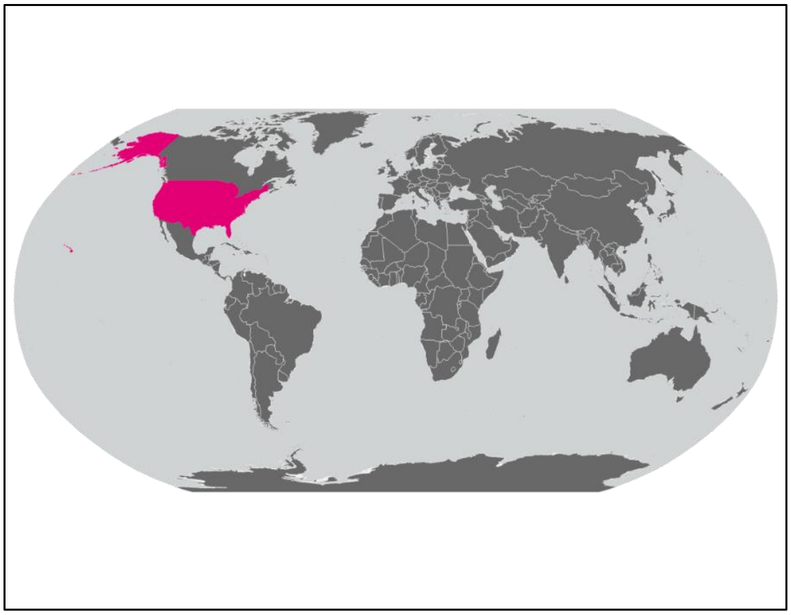


Figure 5.2.1 *NIST Countries*

As highlighted below, the DEVICE passes or at least partially passes **11 or 48%** of the NIST IoT core cybersecurity baseline standards, with **0 or 0%** failures. Figure 5.2.2 and Table 5.2.1 further detail which standards your device meets and what portion of NIST is passed.

NIST REGULATORY MAPPING – DEVICE

8	3	12	0
Pass Evaluations	Partial Evaluations	Unknown Evaluations	Fail Evaluations

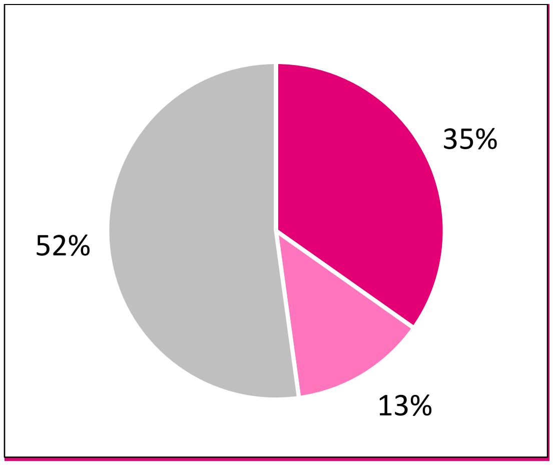


Figure 5.2.2 *NIST Regulatory Mapping*

NIST REGULATORY EVALUATIONS – DEVICE

Category*	NIST Requirement	Evaluation
Device Identification 1	A unique logical identifier	PASS
Device Identification 2	A unique physical identifier at an external or internal location on the device authorized entities can access	UNKNOWN
Device Configuration 1	The ability to change the device's software and firmware configuration settings	UNKNOWN
Device Configuration 2	The ability to restrict configuration changes to authorized entities only	PASS
Device Configuration 3	The ability for authorized entities to restore the device to a secure configuration defined by an authorized entity	PARTIAL
Data Protection 1	The ability to use demonstrably secure cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised	PASS

Data Protection 2	The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cry	**UNKNOWN**
Data Protection 3	Configuration settings for use with the Device Configuration capability including, but not limited to, the ability for authorized entities to configure the cryptography use itself, such as choosing a key length	**UNKNOWN**
Logical Access to Interfaces 1	The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device	**PASS**
Logical Access to Interfaces 2	The ability to logically restrict access to each network interface (e.g., device authentication, user authentication)	**PASS**
Logical Access to Interfaces 3	Configuration settings for use with the Device Configuration capability including, but not limited to, the ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts	**UNKNOWN**
Software and Firmware Update 1	The ability to update the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media)	**PASS**
Software and Firmware Update 2	The ability to confirm the validity of any update before installing it	**PASS**
Software and Firmware Update 3	The ability for authorized entities to roll back updated software and firmware to a previous version	**UNKNOWN**
Software and Firmware Update 4	The ability to restrict updating actions to authorized entities only	**PASS**
Software and Firmware Update 5	The ability to enable or disable updating	**UNKNOWN**
Software and Firmware Update 6a	Configuration settings for use with the Device Configuration capability including, but not limited to: The ability to configure remote update mechanisms to be either automatically or manually initiated for update downloads and installations	**PARTIAL**
Software and Firmware Update 6b	Configuration settings for use with the Device Configuration capability including, but not limited to: The ability to enable or disable notification when an update is available and specify who or what is to be notified	**PARTIAL**
Cybersecurity State of Awareness 1	The ability to report the device's cybersecurity state	**UNKNOWN**
Cybersecurity State of Awareness 2	The ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state	**UNKNOWN**
Cybersecurity State of Awareness 3	The ability to restrict access to the state indicator so only authorized entities can view it	**UNKNOWN**

Cybersecurity State of Awareness 4	The ability to prevent any entities (authorized or unauthorized) from editing the state except for the device's monitor	**UNKNOWN**
Cybersecurity State of Awareness 5	The ability to make the state information available to a service on another device, such as an event/state log server	**UNKNOWN**

Table 5.2.1 *NIST Regulatory Evaluations*

*These category descriptions are not part of the NIST standards and are provided by the Alliance for organizational and reference purposes only.

For a closer look at NIST, the NIST standards, and its valuable resources and publications, visit **here**.

5.3 ETSI Review

ETSI, created in 1988 by the European Conference of Postal and Telecommunications Administrators, is now the officially recognized standards body in Europe dealing with emerging technology, broadcasting, and telecommunication networks. Initially founded in Europe, ETSI has since partnered with countless international organizations to develop standards across the world. Figure 5.3.1 below shows the countries with full ETSI membership.

In June 2020, ETSI released its Cyber Security for Consumer Internet of Thing: Baseline Requirements (ETSI EN 303 645). EN 303 645 provides a set of "outcome-focused" provisions for best security practices in the development and manufacturing of IoT products. The focus on outcome, rather than strict prescriptive rules, gives companies the "flexibility to innovate and implement security solutions appropriate for their products."

This section maps your device against the ETSI provisions.

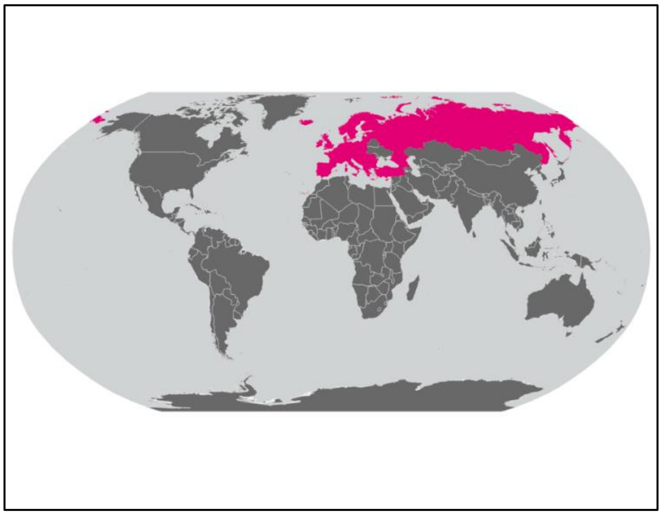


Figure 5.3.1 *ETSI Full Member Countries*

As highlighted below, the DEVICE passes or at least partially passes **26 or 41%** of the ETSI cybersecurity in the Internet of Things standard, with **10 or 16%** failures. Table 5.3.1 and Figure 5.3.2 further detail which standards your device meets and what portion of ETSI is passed.

ETSI REGULATORY MAPPING – DEVICE

26	**0**	**27**	**10**
Pass Evaluations	Partial Evaluations	Unknown Evaluations	Fail Evaluations

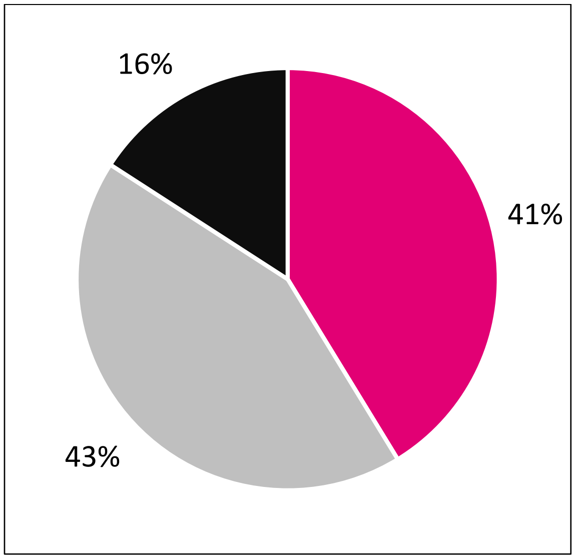


Figure 5.3.2 *ETSI Regulatory Mapping*

ETSI REGULATORY EVALUATIONS – DEVICE

Requirement	ETSI Description	Evaluation
4.0-1	A justification shall be recorded for any provision that is considered to be not applicable for or not supported by the consumer IoT product in question	UNKNOWN
4.1-1	All device passwords shall be unique and not resettable to any universal factory default value	PASS
4.1-2	Where pre-installed passwords are used, these shall be produced with a mechanism that reduces the risk of automated attacks against a class or type of device	UNKNOWN

4.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage	PASS
4.1-4	Where a user can authenticate against a device, the device should provide to the user an easily accessible and intuitive mechanism to change the authentication value used	UNKNOWN
4.1-5	When the device is not a constrained device, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable.	PASS
4.2-1	Provide a public point of contact as part of VDP in order that security researchers and others are able to report issues	PASS
4.2-2	Disclosed Vulnerabilities should be acted on in a timely manner	PASS
4.2-3	Continually monitor, identify and rectify security vulnerabilities throughout the security life cycle	PASS
4.3-1	All software in an IoT device should be securely updateable	PASS
4.3-2	When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates	PASS
4.3-3	The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.	UNKNOWN
4.3-4	The device shall use best practice cryptography to facilitate secure update mechanisms	PASS
4.3-5	Security updates shall be timely	PASS
4.3-6	The device should verify the authenticity and integrity of software updates	PASS
4.3-7	The manufacturer should inform the consumer in a recognizable and apparent manner that a security update is required together with information on the need for that update	PASS
4.3-8	Publish in an accessible way that is clear to the consumer, the defined support period, including the reasons for the length of the period	FAIL
4.3-9	For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer	UNKNOWN
4.3-10	For constrained devices that cannot have their software updated, the product should isolable and the hardware replaceable.	UNKNOWN
4.3-11	An update should be easy to apply and, where possible, automatic mechanisms should be used.	PASS
4.3-12	The device should check after initialization, and then periodically, whether security updates are available	PASS

4.3-13	If the device supports automatic updates, these should be enabled in the initialized state and configurable so that the user can enable/disable/postpone installation of security updates	PASS
4.3-14	The device should notify the user when the application of a SW update will disrupt the functioning of the device.	UNKNOWN
4.4-1	Devices shall store sensitive security parameters securely	FAIL
4.4-2	Where a hardcoded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software	UNKNOWN
4.4-3	Hardcoded critical security parameters in device software source code shall not be used	PASS
4.4-4	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.	FAIL
4.5-1	The consumer IoT device shall use best practice cryptography to communicate securely.	PASS
4.5-2	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography	PASS
4.5-3	When the device is not a constrained device, cryptographic algorithms and primitives should be updateable.	PASS
4.5-4	Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.	PASS
4.5-5	Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication	FAIL
4.5-6	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.	FAIL
4.5-7	The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.	FAIL
4.5-8	The manufacturer should follow secure management processes for critical security parameters that relate to the device.	UNKNOWN
4.6-1	All unused network and logical interfaces shall be closed	FAIL

4.6-2	In the initialized state, the network interfaces of the device should minimize the unauthenticated exposure of security-relevant information.	PASS
4.6-3	HW should not unnecessarily expose access to attack	UNKNOWN
4.6-4	Software services should be removed if they are not used or required by the device.	FAIL
4.6-5	Code should be minimized to the functionality necessary for the service/device to operate	UNKNOWN
4.6-6	Software should run with least necessary privileges, taking account of both security and functionality	UNKNOWN
4.7-1	The consumer IoT device should verify its software using secure boot mechanisms.	PASS
4.7-2	If an unauthorized change is detected to the software, the device should alert the consumer and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.	UNKNOWN
4.8-1	Provide consumers with clear and transparent info about how their personal data is being used, by whom, and for what purposes, for each device/service. Also includes 3rd parties such as advertisers	UNKNOWN
4.8-2	Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way	UNKNOWN
4.8-3	Consumers who gave consent for processing their personal data shall be given the opportunity to withdraw it at any time.	UNKNOWN
4.8-4	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.	UNKNOWN
4.8-5	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.	PASS
4.8-6	All external sensing capabilities (e.g. optic and acoustic) of the IoT device shall be documented for the consumer.	UNKNOWN
4.9-1	Resilience should be built into IoT devices/services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power.	FAIL
4.9-2	IoT services should remain operating and locally functional in the case of loss of network and should recover cleanly in the case of a restoration of a loss of power.	FAIL

4.9-3	Device should be able to return to a network in an expected, operational and stable state in an orderly fashion, rather than in a massive-scale reconnect.	UNKNOWN
4.10-1	Telemetry data from IoT devices/services should be examined for security anomalies	UNKNOWN
4.10-2	The processing of telemetry data from IoT devices/services should be kept to a minimum and such data should be anonymized	UNKNOWN
4.10-3	Consumers shall be provided with information on what telemetry data is collected and the reasons for this.	UNKNOWN
4.11-1	The consumer shall be provided with functionality such that user data can easily be removed from the device.	UNKNOWN
4.11-2	The consumer should be provided with functionality such that personal data can easily be removed from associated services	UNKNOWN
4.11-3	Consumers should be given clear instructions on how to delete their personal data	UNKNOWN
4.11-4	Consumers should be provided with clear confirmation that personal data has been deleted from services, devices and applications.	UNKNOWN
4.12-1	Installation and maintenance of consumer IoT should employ minimal steps and should follow security best practice on usability.	PASS
4.12-2	The manufacturer should provide consumers with guidance on how to securely set up their device.	PASS
4.12-3	The manufacturer should provide consumers with guidance on how to check whether their device is securely set up.	PASS
4.13-1	The consumer IoT device software shall validate data input via user interfaces or transferred via application programming interfaces (APIs) or between networks in services and devices.	UNKNOWN

Table 5.3.1 *ETSI Regulatory Evaluations*

For a closer look at ETSI, the ETSI standards, and its valuable resources and publications, visit **here**.

5.4 ISO Review

COMING SOON

The Alliance is currently developing a new compliance report feature, which will include a regulatory summary and review of International Organization for Standardization (ISO) standards similar to the NIST and ETSI mappings above

5.5 IEC Review

COMING SOON

The Alliance is currently developing a new compliance report feature, which will include a regulatory summary and review of International Electrotechnical Commission (IEC) standards similar to the NIST and ETSI mappings above

5.6 Regulatory News

What's new in IoT standards and regulation? See below for the Alliance's latest digest of regulatory news, trends, and developments in the world of IoT.

ETSI Standard on Consumer IoT Security

With an increasing number of devices across the world being connected to the internet, the security of IoT devices is becoming a larger concern

iot for all ▪ Aug 17

Internet of Things: How the U.K.'s Regulatory Plans Could Raise Compliance Standards

The U.K. government recently launched a consultation process for regulating consumer Internet of Things (IOT) security. This could have significant implications for U.S. manufacturers…

The National Law Review ▪ Aug 12

IoT Governance: How to Deal with the Compliance and Security Challenges

As the IoT becomes more prevalent across an organisation's network, the question of effective IoT governance becomes increasingly relevant

InformationAge ▪ Aug 6

New IoT Security Regulations: What You Need to Know

Over the past few years, the Internet of Things (IoT) market has been experiencing explosive growth. According to Gartner, there will be 25 billion connected devices by 2021

Security Boulevard ▪ Jan 30

IoXt Alliance: Certified IoT Security Program

Certification standards will help manufacturers and using organizations check the certification box on IoT security

no jitter ▪ Aug 14

ETSI Extends IoT Interoperability Specifications to New Areas

ETSI has extended its SAREF IoT interoperability specifications to include automotive, eHealth, wearable and water

ee News Europe ▪ Sept 1

IoTSF Launches Vendor Guides on Consumer IoT Security

The UK based IoT Security Foundation (IoTSF) has launched three guides on consumer IoT security designed to help industry comply with voluntary guidelines and legislation

IoT Australia ▪ Aug 18

US Congress to Mull Legislation Around the Internet of Things
The move comes as China actively seeks to exploit IoT vulnerabilities as well as set technical standards
The Diplomat ▪ Aug 25

NIST Releases Cybersecurity Guidance for Manufacturers of IoT Devices
As a part of its Cybersecurity for IoT Program, NIST recently released two publications with the goal of providing cybersecurity guidance…
The National Law Review ▪ Jun 18

THE
NATIONAL
LAW REVIEW

In addition to the articles above, visit the Alliance's **Blog & Whitepapers** page for more updates and news around IoT regulation and beyond.

6.0 COMPLIANCE TEST REPORT

This section provides a full read out of the DEVICE's compliance report from the ioXt Certification Portal. The DEVICE was certified against the ioXt 2020 Base profile and reached certified status on July 8, 2020.

The following sections are divided into the eight core principles of the **ioXt Security Pledge**:

6.1 VDP – Vulnerability Reporting Program

VULNERABILITY REPORTING PROGRAM – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
VDP1	VDP in place	P		
VDP2	Accept external submission	P		
VDP3	Monitoring security relevant components	N		
VDP4	Responsible disclosures of defects to impacted parties that must take action	N		
VDP5	Public bug bounty program	F		

Table 6.1.1 *Vulnerability Reporting Program*

6.2 SE – Security Expiration

SECURITY EXPIRATION – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
SE1.1	End of life notification policy published	P		
SE1.2	Expiration date is published	N		

Table 6.2.1 *Security Expiration*

6.3 AA – Automatically Applied Updates

AUTOMATICALLY APPLIED UPDATES – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
AA1	Software updates supported	P		
AA2	Software is maintained and updated	P		
AA3	Software updates are made available to impacted parties	P		
AA4	Security updates applied automatically, when device usage allows	P		

Table 6.3.1 *Automatically Applied Updates*

6.4 VS – Verified Software

VERIFIED SOFTWARE – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
VS1	Manufacturer has an update patch policy	P		
VS2	Software images including plug-ins and apps are signed and verified	P		
VS3	Proven cryptography	P		
VS4	Anti-Rollback	P		
VS5	Software images verified at boot time	N		
VS6	Secure boot based on hardware root of trust	N		

Table 6.4.1 *Verified Software*

6.5 PC – Proven Cryptography

PROVEN CRYPTOGRAPHY – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
PC1	Standard cryptography	P		
PC2	Independently reviewed protocol, implementation, or open standard	F		

Table 6.5.1 *Proven Cryptography*

6.6 SI – Secured Interfaces

Compliance tests for all applicable interfaces for the DEVICE:

6.6.1 Ethernet

SECURED INTERFACES, ETHERNET – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
SI1.1	Remote Attack: all certifiable protocols used on the interfaces contained in the device shall be certified	P		
SI1.2	Remote Attack: unused services are disabled	P		
SI1.3	Remote Attack: authentication	P		
SI1.4	Remote Attack: secured communications	P		
SI2.1	Proximity Attack: interfaces are secured against proximity attack	N		
SI2.2	Proximity Attack: authentication	N		
SI2.3	Proximity Attack: secured communications	N		
SI3.1	Local Attack: debug ports are disabled	N		

Table 6.6.1 *Secured Interfaces, Ethernet*

6.6.2 Wi-Fi

SECURED INTERFACES, Wi-Fi – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
SI1.1	Remote Attack: all certifiable protocols used on the interfaces contained in the device shall be certified	P		
SI1.2	Remote Attack: unused services are disabled	P		
SI1.3	Remote Attack: authentication	P		
SI1.4	Remote Attack: secured communications	P		
SI2.1	Proximity Attack: interfaces are secured against proximity attack	N		
SI2.2	Proximity Attack: authentication	N		
SI2.3	Proximity Attack: secured communications	N		
SI3.1	Local Attack: debug ports are disabled	N		

Table 6.6.2 *Secured Interfaces, Wi-Fi*

6.6.3 Zigbee

SECURED INTERFACES, ZIGBEE – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
SI1.1	Remote Attack: all certifiable protocols used on the interfaces contained in the device shall be certified	P		
SI1.2	Remote Attack: unused services are disabled	P		
SI1.3	Remote Attack: authentication	P		
SI1.4	Remote Attack: secured communications	P		
SI2.1	Proximity Attack: interfaces are secured against proximity attack	N		
SI2.2	Proximity Attack: authentication	N		
SI2.3	Proximity Attack: secured communications	N		
SI3.1	Local Attack: debug ports are disabled	N		

Table 6.6.3 *Secured Interfaces, Zigbee*

6.7 SD – Security by Default

SECURITY BY DEFALT – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
SD1	Base security requirements for the profile that the device is being certified under have been met	P		

Table 6.7.1 *Security by Default*

6.8 UP – No Universal Password

NO UNIVERSAL PASSWORD – DEVICE

Test Case #	Test Case Name	Test result (P/F/N)	Additional documentation filename (optional)	Remarks
UP1	Must have user authentication, and must not use common and predictable passwords, or require user to change at initial use	P		
UP2.1	Availability of two factor authentication for devices which have a user facing interface during initialization	N		
UP2.2	Availability of two factor authentication for devices which have a user facing interface during management	N		

Table 6.8.1 *No Universal Password*