MULTI-DIMENSIONAL SECURITY INTEGRITY ANALYSIS OF BROAD MARKET INTERNET-CONNECTED CAMERAS

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

March, 2022

By

Mark A. Stanislav

Dissertation Committee:

Dr. Josh Pauli

Dr. Wayne E. Pauli

Dr. Deb Tech

Dr. Andrea Matwyshyn

Kevin Nassery

DocuSign Envelope ID: B8CA4C7D-3D20-432D-A362-309B021D7CBA

Dakota State University
Completion of Dissertation Final Defense Form

Student Name: Mark Stanislav **Student ID:** A00529686

Title of Dissertation: Multi-dimensional Security Integrity Analysis of Broad Market Internet-connected Cameras

Location of Final Defense: KML 201 / Zoom
Date and Time of Final Defense: March 23, 2022 (**Date**) 2:00pm central (**Time**)

Semester of Intended Graduation: Spring 2022

The above-named student has:

☒ Satisfactorily passed his/her final defense without revisions to the dissertation

☐ Satisfactorily passed his/her final defense with revisions to the dissertation (page 2)

Revisions due:_____
date

☐ Had his/her final defense deferred and will be rescheduled (Please attach letter)

☐ Not satisfactorily completed his/her dissertation defense (Please attach letter)

Signature		Date
	Josh Pauli (co-chairperson)	March 23, 2022
	(co-chairperson)	
Wayne Pauli	Wayne Pauli (member)	March 23, 2022
Deb Tech	Deb Tech (member)	March 24, 2022
Andrea M. Matwyshyn	Andrea M. Matwyshyn (member)	March 28, 2022
Kevin Nassery	Kevin Nassery (member)	March 28, 2022

Completed form will route automatically to:
Dakota State University
Office of Graduate Studies and Research
FAX: 605-256-5093 PHONE: 605-256-5799 E-MAIL: gradoffice@dsu.edu

© Copyright 2022 by Mark A. Stanislav

ALL RIGHTS RESERVED

ACKNOWLEDGEMENT

I would like to foremost highlight the support of my wife, Sarah, and daughter, Edie, over the past many years, through gestures big and small, to help me accomplish this dissertation and all that went before it in my Ph.D. program. Hearing that I was making you both proud made the toughest days approachable and worth it. I love you two very much and value everything you did to help me achieve this goal. This journey was not possible (or meaningful) without your love.

I also want to highlight the decades of support given to me by my parents, Ivan & Mary, who allowed me the space to explore my own forms of learning across my life, even when my traditional school grades sometimes suffered. You prioritized my passion and curiosity, enabling me to not only accomplish three degrees, but do so in my own time and with my own interests.

To my dissertation committee, including my excellent Chair, Dr. Josh Pauli, my long-time friend, Kevin Nassery, my mentor & enabler, Dr. Andrea Matwyshyn, my exceptional teacher & program leader, Dr. Wayne E. Pauli, and Dr. Deb Tech who was kind enough to take a chance on my proposal – thank you all for your support, insights, and time. I hope you are proud of the result. It is a distinct honor to be able to associate this milestone with each of you.

In the spirit of the upbringing that got me here, gr33tz go out to akgood, atanner, c7five, capnal, cje, dpo, dug, eniemann, froggy, hoy, iodboi, jbanfield, jellis, jono, jose, jstrosch, kaospunk, kelby, kimo, lilbunnyfoofoo, mcigna, mfanto, mph, nsoulliere, nwilkens, pinkydancer, pta, quine, radam, redurant, riskin, s7ephen, sally, schlechte, schwascore, sedward5, sfishwick, SilentTension, sirus, slack3r, smoney419, stump, timex, tmanning, todb, tyger, and zajork. Your collective mentorship, inspiration, support, friendship, motivation, and perspective has enabled me to get to this point in my career & academic journey alike. Thank you all for the moments that you each invested in me over the decades; it was not unnoticed or unappreciated.

ABSTRACT

This study used a quantitative approach with a cross-sectional, descriptive analysis survey design to examine the adherence of 40 internet-connected cameras against three IoT security frameworks to determine their overall security posture. Relevant literature was reviewed showing that prior studies in a similar regard had limitations, such as a small sample population, singular market segment focus, and/or a lack of validation against formalized frameworks. This study resulted in a uniform and multi-dimensional set of findings with supporting evidence, leading to a mapping against selected IoT security frameworks that was then quantitatively analyzed for their relative adherence as individual cameras, across market segments, and for the overall sample population. The resultant data provides numerous pervasive gaps in the current state of IoT security that will need to be addressed to ensure consumers are properly protected.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Mark Stanislav

TABLE OF CONTENTS

ACKNOWLEDGEMENT ..... **IV**

ABSTRACT ..... **V**

DECLARATION ..... **VI**

TABLE OF CONTENTS ..... **VII**

LIST OF TABLES ..... **XII**

LIST OF FIGURES ..... **XIII**

CHAPTER 1 ..... **1**

INTRODUCTION **1**

BACKGROUND OF THE PROBLEM 1
STATEMENT OF THE PROBLEM 6
OBJECTIVES OF THE RESEARCHER 7
CONTRIBUTION TO THE DISCIPLINE 7

CHAPTER 2 ..... **8**

LITERATURE REVIEW **8**

THE INTERNET OF THINGS 8
REAL-WORLD IOT CAMERA ABUSE & SECURITY RESEARCH 9
IOT SECURITY FRAMEWORKS & TESTING STANDARDS 15
Industry & Government IoT Security Frameworks *16*
Device Certification *20*
Roll-up IoT Security Publications *21*

CHAPTER 3 ..... **24**

RESEARCH METHODOLOGY **24**

RESEARCH APPROACH & JUSTIFICATION 24
SURVEY SAMPLE POPULATION 26
Sample Size Determination *27*
CREATION OF A CUSTOM ASSESSMENT-TRACKING MECHANISM 31
ASSESSMENT ENVIRONMENT 34
DATA COLLECTION PROCESS 36
Phase 1 – Device Information & Artifacts *37*
Phase 2 – Internal Device Analysis *37*
Phase 3 – Mobile Application Information & Artifacts *37*
Phase 4 – Network Interface Configuration *38*
Phase 5 – Access the Running Device *38*
Phase 6 – Network Service Analysis *38*
Phase 7 – Firmware Upgrade Analysis *39*
Phase 8 – Linux-based OS Analysis *39*
Phase 9 – Privacy Analysis *40*
Phase 10 – Data Completeness & Quality Check *40*
INSTRUMENTATION DETAILS 41
DEVICE EVIDENCE & ARTIFACT COLLECTION 42
LEGAL CONSIDERATIONS 43
DATA COLLECTION LIMITATIONS 43

CHAPTER 4 ..... **45**

RESULTS **45**

OVERVIEW 45
PROPOSED IOT SECURITY FRAMEWORK 46
PROPOSED FRAMEWORK RESULTS 49
Overall Market Segment Analysis 49
Individual Market-segment Analysis 52
Category-based Analysis 63
Control-based Analysis 66
Overall Camera Results 67
DCMS FRAMEWORK RESULTS 71
Overall Market-segment Analysis 71
Individual Market-segment Analysis 72
Control-based Analysis 76
Overall Camera Results 77
ETSI FRAMEWORK RESULTS 80
Overall Market-segment Analysis 81
Individual Market-segment Analysis 82
Category-based Analysis 85
Control-based Analysis 88
Overall Camera Results 89
CAMERA SCORING ROLLUP 91
Data Analysis Questions 93

CHAPTER 5 97

CONCLUSION 97

CONTRIBUTIONS 97
LIMITATIONS 100
FUTURE RESEARCH 104
SUMMARY 105

REFERENCES 107

APPENDICES 120

APPENDIX A: PROPOSED IOT SECURITY FRAMEWORK 120

HARDWARE INTEGRITY (HW) 120
LOCAL ACCESS (LA) 121
MOBILE SECURITY (MS) 122
WI-FI SECURITY (WF) 123
SERVICE SECURITY (SS) 123
HARDWARE SECURITY (HS) 125
FIRMWARE UPDATES (FW) 126
END-USER PRIVACY (EP) 127
BINARY HARDENING (BH) 128
LINUX HARDENING (LH) 129

APPENDIX B: PROPOSED IOT SECURITY FRAMEWORK – CAMERA MAPPING 132

BABY MONITORS 132
CellBee 132
Kami Baby 135
Motorola 137
Sense-U 139
VTech 141
DOORBELLS 143
Energizer 143
Euarne 146
Eufy 148

Victure *150*
Wuuk *152*
HIDDEN CAMERAS 154
Camakt *154*
Ecwey *157*
Pambrum *159*
Swept Supplies *161*
VicZone *163*
PET FEEDERS 165
Didog *165*
HONGSA *168*
IOIODOG *170*
iSmartPet *172*
Sekoya *174*
SECURITY CAMERAS 176
Akaso *176*
Amcrest *179*
Anbes *181*
Anran *183*
Aqara *185*
Conico *187*
DCT *189*
Ecobee *191*
Eversecu *193*
Feit Electric *195*
HeimVision *197*
Jennov *199*
LaView *201*
Mascarry *203*
Moonxiao *205*
Reolink *207*
StartVision *209*
TP-Link *211*
Vacos *213*
WOHOME *215*

APPENDIX C: ETSI – TEST CRITERIA DATA MAPPING 217

APPENDIX D: ETSI – CAMERA MAPPING 221

BABY MONITORS 221
CellBee *221*
Kami Baby *223*
Motorola *225*
Sense-U *227*
VTech *229*
DOORBELLS 231
Energizer *231*
Euarne *233*
Eufy *235*
Victure *237*
Wuuk *239*
HIDDEN CAMERAS 241
Camakt *241*
Ecwey *243*
Pambrum *245*
Swept Supplies *247*

VicZone *249*
PET FEEDERS 251
Didog *251*
HONGSA *253*
IOIODOG *255*
iSmartPet *257*
Sekoya *259*
SECURITY CAMERAS 261
Akaso *261*
Amcrest *263*
Anbes *265*
Anran *267*
Aqara *269*
Conico *271*
DCT *273*
Ecobee *275*
Eversecu *277*
Feit Electric *279*
HeimVision *281*
Jennov *283*
LaView *285*
Mascarry *287*
Moonxiao *289*
Reolink *291*
StartVision *293*
TP-Link *295*
Vacos *297*
WOHOME *299*

APPENDIX E: DCMS – TEST CRITERIA DATA MAPPING 301

APPENDIX F: DCMS - CAMERA MAPPING 302

APPENDIX G: SAMPLE DEVICE FINDINGS 305

BABY MONITORS 305
CellBee *305*
Kami Baby *309*
Motorola *313*
Sense-U *317*
VTech *321*
DOORBELLS 325
Energizer *325*
Euarne *329*
Eufy *332*
Victure *335*
Wuuk *338*
HIDDEN CAMERAS 342
Camakt *342*
Ecwey *346*
Pambrum *350*
Swept Supplies *354*
VicZone *358*
PET FEEDERS 362
Didog *362*
HONGSA *366*
IOIODOG *370*
iSmartPet *374*

Sekoya.....378
SECURITY CAMERAS.....382
Akaso.....382
Amcrest.....385
Anbes.....389
Anran.....392
Aqara.....396
Conico.....400
DCT.....403
Ecobee.....406
Eversecu.....410
Feit Electric.....413
HeimVision.....417
Jennov.....421
LaView.....425
Mascarry.....429
Moonxiao.....433
Reolink.....437
StartVision.....441
TP-Link.....444
Vacos.....448
WOHOME.....451

APPENDIX H: EXTRACTED DEVICE CREDENTIALS.....454

APPENDIX I: ASSESSMENT-TRACKING MECHANISM CONTROL TEST MATRIX.....456

LIST OF TABLES

Table 1. Research survey sample device listing. 29
Table 2. Framework control scoping for assessment-tracking mechanism inclusion. 31
Table 3. Assessment-device instrumentation command list. 41
Table 4. On-sample (Linux) instrumentation command list. 41
Table 5. Proposed framework - market segment control outcome summary. 50
Table 6. Proposed framework - baby monitor control outcome summary. 52
Table 7. Proposed framework - doorbell control outcome summary. 54
Table 8. Proposed framework - hidden camera control outcome summary. 56
Table 9. Proposed framework - pet feeder control outcome summary. 58
Table 10. Proposed framework - security camera control outcome summary. 60
Table 11. Proposed framework - category-based control outcome summary. 63
Table 12. Proposed framework - affirmative testing pass rate, per category, by segment. 65
Table 13. Proposed framework - most common controls for given outcome types. 67
Table 14. Proposed framework - top ten survey devices by affirmative testing pass rate. 68
Table 15. Proposed framework - top ten survey devices by absolute testing pass rate. 69
Table 16. Proposed framework - top ten survey devices by absolute testing failure rate. 69
Table 17. Proposed framework - top ten survey devices by affirmative testing failure rate. 70
Table 18. DCMS - baby monitor control outcome summary. 73
Table 19. DCMS - doorbell control outcome summary. 73
Table 20. DCMS - hidden camera control outcome summary. 74
Table 21. DCMS - pet feeder control outcome summary. 74
Table 22. DCMS – security camera control outcome summary. 75
Table 23. DCMS – summary by control outcome. 76
Table 24. DCMS - top 13 survey sample devices by outcome pass rate. 79
Table 25. DCMS - bottom eight survey sample devices by outcome pass rate. 80
Table 26. ETSI - baby monitor control outcome summary. 82
Table 27. ETSI - doorbell control outcome summary. 83
Table 28. ETSI – hidden camera control outcome summary. 83
Table 29. ETSI - pet feeder control outcome summary. 84
Table 30. ETSI - security camera control outcome summary. 85
Table 31. ETSI - category-based control outcome summary. 86
Table 32. ETSI - top-and-bottom ten survey sample devices by outcome pass rate. 89

LIST OF FIGURES

Figure 1. Security control-to-categorization mapping totals. 32
Figure 2. Assessment environment diagram. 34
Figure 3. Proposed framework - control outcomes by market segment. 51
Figure 4. Proposed framework - control outcomes for baby monitors by vendor. 53
Figure 5. Proposed framework - control outcomes for doorbells by vendor. 55
Figure 6. Proposed framework - control outcomes for hidden cameras by vendor. 57
Figure 7. Proposed framework - control outcomes for pet feeders by vendor. 59
Figure 8. Proposed framework - control outcomes for security cameras by vendor. 62
Figure 9. Proposed framework - control outcomes by control category. 64
Figure 10. Proposed framework - affirmative pass percentage, per category, by segment. 66
Figure 11. DCMS - control outcomes by market segment. 72
Figure 12. DCMS – control outcomes by control identifier. 77
Figure 13. DCMS – device count by passing outcome percentage. 78
Figure 14. ETSI - control outcomes by market segment. 81
Figure 15. ETSI - control outcomes by control category. 87
Figure 16. ETSI - pass percentage, per category, by segment. 88
Figure 17. ETSI - control outcomes by vendor. 90
Figure 18. Aggregate framework pass rate by vendor. 91
Figure 19. Aggregate framework pass rate by market segment. 92
Figure 20. Aggregate framework pass rate by device price. 94
Figure 21. Aggregate framework pass rate for vendors with a security policy. 95
Figure 22. Aggregate framework pass rate by vendors making security claims. 96

CHAPTER 1

INTRODUCTION

Background of the Problem

The rapid growth of Internet of Things (IoT) devices in the market (Newman, 2020) is accelerating a conversation among consumers as to whether the value of such offerings can be balanced against the potential risks to their privacy, safety, & security. For vendors to be on the favorable side of that balance, consumers must place trust in the device and associated service ecosystem being offered to them. Trust in this context can be defined as, "a willingness to be vulnerable to another party" (Schoorman, Meyer, & Davis, 2007). This perception of trust as related to IoT can be further qualified as requiring consumers to hold "beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible" (McKnight, et al, 2011).

Currently, however, consumers may not have the level of trust in such devices as those vendors would prefer. In an academic study from the United Kingdom, researchers concluded that, "consumers expect that their security could be at risk and that security incidents would have a fairly significant impact" (Cannizzaro, et al., 2020). Another consumer study found that only 9% of respondents had trust in the way that IoT devices collected and shared data (Cisco, 2017).

As noted by academic IoT researcher AlHogail, "an IoT system must possess a series of characteristics, such as encryption and usefulness, in order to be trusted and accepted by users" (2018). Unlike a typical consumer computing purchase (e.g., tablet, laptop, cell phone), the devices that make up the broader IoT landscape lack the ability to install familiar security

enhancements (e.g., anti-virus, firewalls) and limit the amount of direct interaction a user has with it to implement their own security improvements. The opaque-by-design nature of these utilitarian embedded devices only serves to distance a consumer's feeling of control as to what is going on inside of their purchase.

Consumer trust is further eroded with news stories highlighting the potential risks for an insecure IoT device in their home. The creation of a botnet called Mirai was initially formed with over a half million IoT devices co-opted by criminals to attack numerous parts of the internet (Bursztein, 2017). Similar types of IoT-focused botnets have been created since then, including Kaiten & Qbot (Hilt, Mercês, Rosario et al., 2020). Unlike a personal computer, which may detect a compromise of its system, or exhibit unexpected behaviors leading to an investigation by professionals, IoT devices are effectively "black boxes" as to what sort of abuse may be occurring. A consumer may only realize that their IoT device has been compromised for such abuse if contacted by their internet service provider (ISP) or law enforcement to inquire why they are conducting an attack against a web service.

Not all IoT device attacks are silent, however, as is often the case when a home's smart camera is hijacked by someone over the internet. In one case, a family was harassed through the smart camera that was placed in their baby's room with threats that the attacker would kidnap their child (Rascon & Aragon, 2018). More recently, a criminal group has claimed to have hacked more than 50,000 internet cameras from around the world with recordings accessible to purchase online (Sun, 2020). Even more troubling, however, is a more recent alert put out by the Federal Bureau of Investigation (FBI) that hacked cameras are being used to bring law enforcement to a home under false pretenses (e.g., domestic dispute) and then use that same device to communicate with the police (Federal Bureau of Investigation, 2020). Such activity is

part of a larger internet-driven prank known as “swatting” that has led to actual deaths (Brice-Saddler, et al., 2019) and is only increased in effectiveness when internet-connected microphones, speakers, & cameras are involved. These technologies bridge the implicit gap of online abuse from the digital to the physical, changing the potential for harm in profound ways.

Consumers may also struggle to put trust into an IoT product due to the opaqueness that is inherent in most offerings. If a customer of an eBay auction purchases an IoT baby monitor from a seller – even marked “new in box” – how does that purchaser really know that the device has not be tampered with? Unfortunately, vendors may fail to limit such abuse cases through basic methods like disabling debug interfaces (Praetorian, 2016) or by simply adding tamper-evident stickers to the device’s enclosure (Grand, 2004). Devices may also accept firmware updates over insecure network protocols, like Telnet, or do not require authentication, as was the case with Hasbro’s Bluetooth-enabled Furby device (Ferreira, 2017). With used/open-box goods from Amazon or Best Buy, an internet-based attacker may be the least of a consumer’s worries when an entire device can be compromised before it is delivered.

In guidance around securing IoT devices from attacks like the examples, basic password security is a common topic (Teller Vision, 2017). This guidance is necessary due to a common practice by IoT vendors of selling devices that have a pre-configured password that consumers do not change when setting it up for the first time (Consumers International and Internet Society, 2018). In other cases, IoT vendors use what are considered hardcoded passwords because the consumer cannot change them, even if they wanted to (Vamosi, 2014). This guidance is valuable to consumers, of course, but it only begins to look at the complex set of risks that consumers must manage when considering the enormity of a single device’s ecosystem, including radios,

firmware, system services, cloud services, mobile applications, physical security, cryptography, & network protocols (Lanier & Stanislav, 2014).

To have trust in an IoT device, integrity of given security mechanisms must exist. When a hardcoded password is used, for instance, there is no way to ascertain if the authentication of that account belongs to the device owner instead of an attacker. The same can be said for any part of an IoT device, such as firmware update processes. In one case, a security researcher named Mike Davis found that the vendor Belkin had accidentally released the cryptographic private key that was used to provide authenticity to firmware updates, allowing an attacker to create their own valid signature and install malicious updates on relevant devices (Fisher, 2014). Another example of weak integrity of intended security controls can be seen from research conducted by the firm Bitdefender who noted that Amazon's Ring doorbell would send a home's Wi-Fi network password unencrypted during configuration, allowing for a nearby attacker to intercept it, reducing the home's overall network security beyond the device (Whittaker, 2019).

As instances of poor IoT security made international headlines, the U.S. federal government started to act towards setting a tone that such lapses are not in consumers' interests. The Federal Trade Commission (FTC), for instance, filed a complaint against the vendor TRENDnet, Inc. due to their lack of security controls that allowed criminals to easily access hundreds of internet-connected cameras they sold (Federal Trade Commission, 2014). This complaint ultimately led to a settlement that required actions by TRENDnet, including the establishment of a comprehensive security program, having third-party security assessments every two years, and restricting their ability to make statements on the security of their devices in materials to consumers, such as advertisements or manuals (Federal Trade Commission, 2014).

The Consumer Product Safety Commission (CPSC) held a panel hearing about IoT safety (*The Internet of Things and Consumer Product Hazards*, 2018) that ultimately led Elliot Kaye, one of the commissioners of the CPSC, to publish a framework for IoT safety (Kaye & Midgett, 2019). Just recently, the U.S. government passed a new law (IoT Cybersecurity Improvement Act of 2020) to bring federal attention to codifying recommendations via the National Institute of Standards and Technology (NIST) on how such devices must be secured. While such laws set a tone of urgency and importance, many existing security standards, frameworks, guidance documents, and expectations for IoT security already exist today.

In 2014, the international security consulting firm, NCC Group, published a paper titled, "Security of Things: An Implementer's Guide to Cyber Security for Internet of Things Devices and Beyond" that discussed in depth the threats, threat actors, risks, and proactive approaches to the broader view of IoT security integrity (Whitehouse, 2014). The following year, the "Internet of Things Trust Framework" was released by an industry consortium called the Online Trust Alliance (OTA) that represented expertise in security & privacy from over a hundred participating individuals, organizations, and companies (Online Trust Alliance, 2015). In 2016, an organization called the IoT Security Foundation (IoTSF) released a document called the "IoT Security Compliance Framework" that covered thirteen compliance categories spanning a broad set of security & trust topics (IoT Security Foundation, 2016). Additional IoT security guidance documents are still being released to this day from industry organizations (Cloud Security Alliance, 2019) and governments, including the United Kingdom (U.K. Department for Digital, Culture, Media & Sport, 2018) and an in-progress draft from India (India Telecommunication Engineering Center, 2020). While the U.S. federal government has made a specific choice to

bring attention to IoT security in the way of a law, the guidance that NIST ultimately ends up providing may end up looking like the numerous documents that have gone before its own.

What's not clear to consumers, however, is how much these industry and governmental standards have influenced the way vendors are building their IoT devices today. While there are efforts by organizations, such as UL, to perform IoT security certification of devices (UL, 2019). This approach is still in its nascency and will mostly address the needs of larger, more financially stable vendors who can afford to purchase this service. This reality leaves a gap in empirical security testing of devices – on scale – for consumers to determine if recent IoT devices are appropriately maximizing years of security guidance. If consumers are expected to increase their trust in IoT, analysis of the current state of IoT devices in each market segment – a process of dividing up a mass market into groups with similar needs and wants (Pride et al., 2018) – must occur to determine how much of the guidance from years past has been used in practice.

Statement of the Problem

The Internet of Things is generally valued in usefulness, but also generally deemed untrustworthy for security, by consumers in the market (Cisco, 2017). With ongoing news stories covering compromised IoT cameras, ranging from baby monitors (Rascon & Aragon, 2018) to doorbells (Whittaker, 2019), trust will be difficult to establish without a holistic approach to securing these powerful devices. While numerous IoT security frameworks have been released (Online Trust Alliance, 2015; IoT Security Foundation, 2016; Cloud Security Alliance, 2019; U.K. Department for Digital, Culture, Media & Sport, 2018), consumers are unaware if that guidance has been realized in the devices of today's market. Previous research on IoT camera security has been too shallow in security control assessment & device sample size (Stanislav & Beardsley, 2015; Alharbi & Aspinall, 2018) and did not reflect industry frameworks & standards.

Objectives of the Researcher

In response to the problem, this study sought to investigate how recent IoT cameras have addressed holistic security concerns as defined by published IoT security frameworks. This research has made the following contributions:

1. A multi-dimensional security-integrity analysis – involving a technical assessment of industry-standardized security controls across IoT ecosystem components – of 40 connected cameras that are representative of the broader market, including security cameras, baby monitors, doorbells, pet feeders, & hidden cameras.

2. Mapping of assessed IoT camera security properties against two published IoT security frameworks that define their own criteria for what makes such a device secure.

3. Quantified adherence of each assessed device against the chosen IoT security frameworks to determine whether vendors are meeting such guidance in practice.

Contribution to the Discipline

This research sought to contribute a current, representative, and detailed analysis of internet-connected camera security adherence to widely published IoT security standards. Industry professionals, vendors, academics, and consumers alike will be able to determine if the broader IoT camera market space is maximizing the published guidance on providing secure products to the market, helping to assert whether consumer mistrust is warranted. Additionally, data generated from this research study enables other researchers to draw their own conclusions about the state of IoT security as represented by the survey's sample device findings.

CHAPTER 2

LITERATURE REVIEW

In Chapter 2 we explore a literature review that covers the foundations of IoT camera security, including the research history of such devices, abuse cases in the real world, and prior studies that attempt to qualify cameras on the market for appropriate security rigor. The current state of IoT security frameworks & standards will also be analyzed to highlight the amount, approach, and variance in guidance available to IoT device manufacturers for security practices.

The Internet of Things

While definitions for the Internet of Things (IoT) can vary widely, the International Telecommunication Union (ITU) has defined a set of characteristics including interconnectivity, things-related services, heterogeneity, dynamic changes, and enormous scale (International Telecommunication Union, 2012). This broader term can then be broken down into more domain-specific instantiations of these characteristics, such as the smart home market. A smart home is defined by the ITU as a "system that consists of embedded communication devices, including home appliances, home energy equipment, and various sensors within and around the home, for the purpose of data collection and equipment control" (International Telecommunication Union, 2015).

Of the broader smart home market, numerous camera-related types exist, including security cameras, baby monitors, doorbells, pet feeders, & hidden cameras. While the product marketing, form factors, and feature set of such devices may differ across these product

categories, they all share the ability to observe their installed location and create a video stream that can be used as necessary. Such devices represent non-trivial global market segments with spending for IoT security cameras representing $3.9B (Grand View Research, 2020) and IoT baby monitors forecasted to reach $1.7B by 2025 (Grand View Research, 2019).

Real-world IoT Camera Abuse & Security Research

While the Internet of Things designation has become popular in recent years, the phrase dates to 1999 when an employee working at Proctor & Gamble coined it while working on a supply chain project using a radio frequency identification (RFID) based technology (Postscapes, 2019). Similarly, standalone internet-connected cameras, while far more ubiquitous today, have been available to consumers for decades now. In 2002, D-Link released the DCS-1000w, featuring both Wi-Fi and Ethernet connectivity (Schwartz, 2002). Also made available that year was the 2100 Network Camera model from the vendor Axis (Axis, 2002). This camera, unfortunately, had severe security defects that allowed a remote attacker to read and edit files hosted on the camera (Bashis, 2004). Three years later, security researchers used this same camera to highlight their ability to hijack the video stream of this camera and instead show a pre-selected video of their choice to the owner (Singel, 2007). Similar research was performed by a different security researcher, Craig Heffner, six years later, exploiting numerous cameras while also highlighting a video stream hijack (Rubenking, 2013).

When such issues arise, their abuse can be combined with otherwise harmless technologies, such as search engines, to exasperate the risk through ease-of-discovery by attackers. Dating back at least 20 years (Greene, 2000), the idea of using search engines to find web servers with abusable functionality has found fertile ground with internet-connected devices in crafting so-called “Google Dorks” (Long, 2002). Due to the advanced indexing of many

search engines, queries can filter partial strings in a web server's URL or other meta data that will allow a surgical analysis of indexed sites to find those which may in fact be connected devices. In the case of internet-connected cameras, many of them have a built-in web server to provide the owner a way to administrate functionality and view the stream of the device. These queries can be run manually to target specific cameras or may become aggregated into indexes.

The website camhacker.com was started in 2006 to index internet-exposed cameras in a manner that lets anyone – without needing technical knowledge or even Google search queries – to discover streams that do not require authentication to see their contents (CamHacker, 2019). In more recent times, exposures have been broadcast via dedicated Twitter bots (Paganini, 2016) or made even easier to find with internet scanning tools, such as Shodan.io. In 2012, a notable event in this space occurred with a security research group calling themselves, Console Cowboys, who published a blog post detailing the discovery that their TRENDnet TV-IP110w could be accessed remotely without authentication (Console Cowboys, 2012). That initial post led to over a thousand such cameras being indexed onto the text sharing website, Pastebin, for people to scour within just days (Notopoulos, 2012). The TRENDnet story did not stop there, however, as a year later a Twitter account called TRENDnetExposed began to share actively exposed cameras, along with a map web page showing the approximate location of those devices (Toor, 2013).

In 2014, a new exposed camera indexing site called Insecam.com represented itself as having over 73,000 indexed cameras (Biggs, 2014). Unlike previous situations where a web server was simply missing appropriate authentication, this site took abuse one step further by also indexing devices that use default and hardcoded passwords, too (Smith, 2014). This site still exists but appears to only index sites that do not require any password now – like what a user can do searching on Shodan.io. As of February 2021, there were over 10,000 cameras indexed

globally, representing dozens of vendors, including over 3,800 in the United States alone (Insecam, n.d.). While some of these cameras are surely intending to be public, users of these sites have no way to know who has intended to provide authorization to view a camera or not. While the numbers are large, Alex Balan from the security firm Bitdefender published research in 2017 that identified security issues in two cameras that had approximately 130,000 known internet exposures (Franceschi-Bicchierai, 2017), highlighting the potential scale of abuse when large manufacturers have a mass-market presence with insecure technology.

Beyond general-purpose connected cameras, the subject of internet-connected baby monitors has been of particular focus in recent years, but large-scale concerns date back much further. In 2013, security researchers at Shape Security & Qualys identified multiple issues with the IoT vendor Foscam, leading them to find over 40,000 abusable baby monitors (Hill, 2013). Not long after that research was published, a family in Texas reported that someone used their home's camera to say offensive things to their 2-year-old child with the belief that the findings from the previous research were likely used to perform that abuse (Hill, 2013). In that case, the vendor had attempted to fix issues, but most of the impacted devices were still not updated. Similar stories have occurred in Ohio (FOX19, 2014), Ontario (Ingram, 2015), New York (Jiang, 2015), and Tennessee (Holley, 2019) over the years. A research study by the security firm Rapid7 further highlighted risks to internet-connected baby monitors with vulnerabilities that could allow an attacker take control of devices over the internet or steal previously recorded videos from cloud storage providers used by the vendors (Stanislav & Beardsley, 2015).

Regardless of the type of camera, similar concerns are present. A vulnerability analysis by security researcher Mike Davis highlighted network security issues with a Wi-Fi enabled pet camera from the vendor Petcube (Davis, 2015). Connected doorbell hacking has even led to law

enforcement officers surrounding a home, speaking to a so-called “prankster” that was remotely impersonating the homeowner through their Ring doorbell (Federal Bureau of Investigation, 2020). Devices of any form or function that contain a camera – and additional features like microphones & speakers – offer the same risks to the consumers that install them. While the location of a baby monitor and a doorbell are quite different in practice, their proximity to users and ability to connect to the same network as the rest of a family’s computers contain a non-trivial risk to privacy, safety, and security when not appropriately secured.

Beyond privacy risks, internet-connected cameras have also been used by attackers in large-scale botnets to harm internet services. Abuse at this level has been increasing as have the opportunities for attackers to amass the computing & network power to achieve desired outcomes, whether for financial or destructive goals. Of most notable fame, the Mirai botnet conducted a DDoS attack of approximately 620Gbps, which exceeded the largest previously seen attack by almost double – and did not use amplification to do so unlike the prior record (Krebs, 2016). This number only grew in subsequent attacks, with a near-doubling again of 1.1Tbps (Goodin, 2016). The next month, in October 2016, the Mirai botnet took down the DNS provider, Dyn, having an impact on major sites like Netflix, Twitter, and Amazon (Krebs, 2016). This botnet was comprised of IoT devices of all sorts – including cameras – using hardcoded and default credentials to gain direct OS-level access to their hardware. Other botnets have been created in a similar approach and impact, such as Persirai which involved over 120,000 internet-connected cameras across more than 1,000 individual device models (Palmer, 2017).

The security researcher Rob Graham put an IoT camera online that he had purchased to see how fast it may be compromised; that wait took only 98 seconds (Smith, 2016). Once the initial compromise occurred, Graham stated that additional malware payloads were installed and

started to try and infect other portions of the internet. This sort of expediency of compromise means that most consumers would have no real chance to update insecure firmware – if such an update even existed – before the device would already be compromised. The potential of such abuse of devices gets even more serious when considered in context to reports that the Russian Federal Security Service (FSB) had an initiative dubbed "Fronton Program," targeting IoT devices (Doffman, 2020).

These kinds of exposures have led to multiple complaints by the United Stated Federal Trade Commission (FTC), including against TRENDnet in 2014 (FTC, 2014) and D-Link in 2017 for their own failure to appropriately secure sold internet-connected cameras (FTC, 2017). An additional investigation by New York's Department of Consumer Affairs (DCA) was also launched in 2016 due to the documented research and abuses of internet-connected baby monitors, including subpoenas to four vendors (Greenberg, 2016). More recently, a class-action lawsuit was filed by four plaintiffs against Ring for the lack of security controls available to customers to secure their devices from the types of abuses that have occurred via internet-connected cameras (Bell, 2020).

Comprehensive academic research on the topic of internet-connected camera security has been rather minimal to date, with only a couple of papers focused on detailed technical analysis across a multiple-device sample. Building on previous industry research, Bugeja, et al, explored what types of internet-connected cameras were readily available for abuse, including those that had previously known vulnerabilities (2018). In their results, the authors noted over 500,000 devices found running a popular embedded web server that is common on connected cameras. An additional 78,000 devices were discovered in their usage of keywords associated to filters on the Shodan.io device search engine service. This paper furthers the awareness that internet-

exposed cameras are rampant but does not add to the literature any specific new risks, approaches, or market-based conclusions about internet-connected devices beyond what has been explored in prior research reports.

Perhaps the most robust academic IoT camera study as it relates to drawing conclusions around the security maturity of devices in the market comes from Alharbi & Aspinall in their paper, "An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities" (2018). The authors have taken an approach to define elements of security, as specified in 13 test cases, that attempt to highlight more robust IoT ecosystem security. This analysis framework drew inspiration from multiple sources, including OWASP & IEEE guidance, but does not attempt to leverage any existing frameworks in full that were available at the time of research. Their research covered five cameras in total, including Ring, Neatmo, & BT, with findings being documented as descriptive text in their report. While they refer to their analysis approach as test cases, the work is more appropriately labeled as testing areas in practice.

In their analysis, Alharbi and Aspinall ultimately qualify their test case results in a variety of ways that vary from camera-to-camera. Unlike a detailed testing framework that will enumerate potentially hundreds of specific tests, the open-ended nature of their analysis means that a given camera may be marked as *red* (i.e., a severe issue) for a variety of reasons, making it hard to compare cameras uniformly to one-another. If the authors had broken out their 13 test cases into sub-cases, there would have been more clarity as to the relative risks highlighted. The authors also qualify *positive* security found in devices, but do so with troubling language such as, "Good certificate parameter," as was the case with the Ring Doorbell's use of application signing. Having more discrete criteria would have allowed them to note such positive facets of a device, but in more of a true/false qualification, yielding data that was simpler to compare.

Ultimately, the IoT analysis framework proposed by the authors of this paper fall into the same trap as much of the industry – creating yet-another partial approach to a topic that has numerous robust and detailed testing approaches already. The methodology and assessment of their work does highlight, however, the value in performing comparative analysis of devices in a similar segment space to shine a light on the strengths and weaknesses of the market. Improvement upon their work would involve a more robust sample size, make use of existing frameworks, breakdown assessment criteria granularly, and assert more one-to-one analysis.

IoT Security Frameworks & Testing Standards

In the broader field of information security, professionals have come to rely on industry organizations, working groups, and government agencies to codify approaches that help to ensure a given system has appropriate controls. A control is defined as a "measure that is modifying risk" (International Organization for Standardization, 2018). An organization wishing to mature their security may, for instance, use a publication by National Institute of Standards and Technology (NIST) called the "Cybersecurity Framework," which provides a structured approach to information security spanning 108 control areas (National Institute of Standards and Technology, 2018). In practice, many such frameworks & standards are tied more to an organizational security program, rather than a technological product. This leaves an alignment gap between well-known offerings (e.g., SOC 2, ISO 27001) and the needs of an IoT device. To address this gap, numerous organizations and governmental bodies have taken it upon themselves to devise IoT-specific security frameworks that desire to mature the market.

Industry & Government IoT Security Frameworks

One of the earliest efforts to codify IoT security was the publication, "Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond," which was the work of the global information security firm, NCC Group (Whitehouse, 2014). Of note, this document was structured across six phases of the IoT product lifecycle, covering design, requirements, architecture, implementation, verification, & maintenance. Phases three, four & five, tables of requirements, descriptions, and reasonings are provided with longer-form, more descriptive content to highlight areas of interest ranging from technical to business operation aspects of a secure IoT device lifecycle. There are 82 stated considerations across hardware, software, architecture, implementation, and verification topics, many of which are very technical and specific, such as "Vias provide an attack service to the circuit board. As a result, their exposure should be considered, and possible attacks mitigated. Where possible, blind and buried vias should be used" (Whitehouse, 2014). Because of the firm's security research background, the guidance found in this document, even seven years later, considers much of the attack surface at a more granular level than many recent frameworks.

In 2015, The Online Trust Alliance (OTA), which is an initiative of the Internet Society, created the IoT Trustworthy Working Group (ITWG) to leverage a cross-industry collaboration of more than 100 organizations to build what became the IoT Trust Framework (Online Trust Alliance, 2015). In defining what such a framework may involve securing the nascent world of IoT, the ITWG leveraged existing security guidance from organizations such as the Federal Trade Commission (FTC), International Association of Privacy Professionals (IAPP), and the Open Web Application Security Project (OWASP) to maximize prior art more quickly. The first official release of the framework, v1.0, was released in March 2016 (Help Net Security, 2017) and originally included thirty technical guidelines split into the categories of "security," "user

access & credentials," and "privacy, disclosures, & transparency" (Online Trust Alliance, 2016). The guidance was also mapped to contexts of "connected home" and "wearables" (e.g., smart watches) with listed guidelines having a "required," "recommended," or "not applicable" designation. The last release of the IoT Trust Framework, version 2.5, came out in October 2017 and had by then extended to 40 guidelines across four categories (Online Trust Alliance, 2017).

The IoT Trust Framework takes the approach of collapsing multiple recommendations into larger technical guideline sections, resulting in less specific guidance. For instance, one partial guideline starts with, "Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices" (Online Trust Alliance, 2017). As a framework, the reader is still left to figure out how this applies to their specific product, which can vary widely depending on what sort of cryptographic protocols are applicable. Other parts of the framework address subject matter far beyond technical controls, such as business-level communication plans in the event customers need to be made aware of a security vulnerability. The IoT Trust Framework is therefore robust in a breadth of subject matter sense, but the low specificity of many guidelines means that vendors will typically have the general idea of what to do, but not exactly how to do it. As the framework is no longer being updated, this also leads to a situation where times goes on, guidance may become less accurate.

A more action-oriented approach to the subject of IoT security is the OWASP "IoT Security Verification Standard (ISVS)," which is a community project aimed to define actual testing steps to take for a given IoT device to ensure appropriate security properties exist (Guzman & Bassem, 2021). As of the time of writing, this document is still in a release candidate stage. The OWASP ISVS provides rather specific guidance on what to observe within a given device as to whether-or-not appropriate security properties are in place, rather than describing the

conceptual risks that need to be managed for. Where other control-focused frameworks may explain the context of a risk, the OWASP ISVS focuses more attention on the outcomes.

The document breaks down technical categories into “IoT ecosystem,” “user space application,” “software platform,” “communication,” and “hardware platform,” covering approximately 125 assessment criteria associated to three levels of verification. Devices being assessed will have variable levels of applicability as the technologies, protocols, and implementations covered may simply not be used by a given IoT device. Other criteria, such as, “verify that packages and user space applications use over the air updates decoupled from firmware updates” (Guzman & Bassem, 2021) is an opinionated design choice by the document’s authors, rather than a universally accepted norm of how security must be implemented. Because of the verification focus of the document, the *why* of an assessment step is left up to interpretation.

In a more robust offering, the IoT Security Foundation (IoTSF) first released their “IoT Security Compliance Framework” in 2016, which has since been update to version 2.1 as of May 2020 (IoT Security Foundation, 2020). To meet the broader ecosystem needs of an IoT device, this framework chooses to breakdown assessment criteria into numerous sub-groups, including “business process,” “device hardware,” “device software,” “device OS,” “device interfaces,” “authentication & authorization,” “encryption & key management,” “web user interface,” “mobile application,” “privacy,” “cloud and network elements,” “secure supply chain production,” “configuration,” and “device ownership transfer.” Across these 14 focus areas there exists a total of 240 requirements that each associate to one-or-more classes of compliance with a *mandatory* or *advisory* applicability.

In this structure, the framework can more specifically break down requirements that may otherwise be ambiguous in terms of applicability, such as security around secure transports, where in the OTA's framework, such topics were generalized for all contexts without specificity. Like OWASP ISVS, IoTSF's offering has a mixture of very prescriptive guidance (e.g., "The product does not accept the use of null or blank passwords.") with very vague guidance (e.g., "In systems with many layered sub devices, key management should follow best practice.") interspersed (IoT Security Foundation, 2020). While the 240 requirements are far larger than the IoT Trust Framework (30) or the OWASP ISVS (125), many of the statements are referential to using other existing standards or repeating the *best practices* phrasing in many requirements.

The United Kingdom's Department for Digital, Culture, Media, & Sport (DCMS) released the "Code of Practice for Consumer IoT Security" during October 2018 to distill down the analysis of approximately 100 documents from nearly 50 resulting in 13 practices (U.K. Department for Digital, Culture, Media & Sport, 2018). Where other documents create a detailed framework, the DCMS instead chose to simplify the number of topics to tackle with relatively short descriptions that are less prescriptive and targeted than other documents in the space. The document further qualifies those practices by associating them to whether they are applicable to one-or-more focuses of "device manufacturers," "IoT service providers," "mobile application developers," and/or "retailers." In this approach the DCMS went more towards the path of the OTA's "IoT Trust Framework" in avoiding hundreds of discreet, technical controls in favor of focusing attention on more pressing topics (e.g., "No default passwords") that while not novel in their concern, are targeting more pervasive and impactful risks that are avoidable. As a standalone artifact, it is sufficient to help guide an IoT vendor but would need to use many of the original source inputs to fully capture the depth of guidance.

In March 2019 during the RSA Conference, the Cloud Security Alliance (CSA) released the "CSA IoT Controls Framework" that was created by an organizational working group specifically for Internet of Things initiatives (Cloud Security Alliance, 2019). Spread across 26 control domains are 180 total controls with each being associated to an impact level of *low*, *moderate*, or *high*. Notably, the CSA provides context around the type of control (e.g., preventative), the frequency of its use (e.g., quarterly), and an implementation method (e.g., automatic) that other frameworks do not share. This means that the CSA is taking a more robust look at the ongoing lifecycle management of security instead of point-in-time validation. The lens of these control domains is more generalized (e.g., credential management) rather than focusing on an implementation case (e.g., operating system), which broadens the applicability for any given control to the ecosystem, rather than a single use case. The framework has another novel structural element, which is using the IoT component context to associate controls more directly, such as defining what is applicable to a sensor, versus the mobile application, versus a cloud service provider involved.

Device Certification

Device certification programs also have the concept of an IoT security framework built into them, such as the CTIA's "Cybersecurity Certification Program for IoT Devices," covering three possible levels of certification for a given device (CTIA, 2021). CTIA first established this certification program in October 2018 as an expansion from their larger focus in wireless testing (CTIA Certification, 2018). The testing criteria for IoT is spread over nineteen functional areas that are variably applicable, depending on the level of certification chosen by a vendor to pursue (CTIA, 2021). The "Level 3 IoT Cybersecurity Tests," for instance, will have approximately forty-five procedures that must be met, as applicable to the device's functionality, and mapped to

several higher-level requirements. A testing requirement also provides prerequisites when necessary, so that there is guidance on how to configure a device so that, when the testing occurs, it is more likely to yield the expected outcome accurately.

Another IoT device certification comes from UL (f/k/a Underwriters Laboratories), which in June 2019 established their own program using a 5-level verification standard (UL, 2019). Across seven categories, a total of 43 requirements exist that are then mapped to one-or-more of the certification levels that span technical and process facets around that IoT device. In the case of the first level of certification, *Bronze*, only 11 of 43 requirements are in scope, limiting expectations to what may be considered basic security (e.g., software updates, not having default credentials) for an IoT device. A notable difference in UL's approach versus other testing frameworks is that they use terse requirement titles with larger – sometimes multiple paragraph – explanations of guidance that is broadly descriptive instead of prescriptive. This broader description provides latitude for a given device assessor to use the intent of the requirement more than a single checkbox to discern adherence. This can be a positive, depending on the expertise of the assessor, to allow for a more thoughtful analysis of the testing, but also creates a scenario that may yield inconsistent test results across devices.

Roll-up IoT Security Publications

A different take on the roll-up style security framework for IoT is a derivative effort by the Council to Secure the Digital Economy (CSDE) called "The C2 Consensus on IoT Device Security Baseline Capabilities" (Council to Secure the Digital Economy, 2019). In this effort, the CSDE, "brought together trade associations, standards development organizations, industry alliances and coalitions to develop the C2 Consensus Baseline, the broadest and most technically

deep industry consensus on IoT security worldwide" (Council to Secure the Digital Economy, 2019) including CTIA, UL, and others referenced prior.

In total, there are only 13 listed "Consensus Baseline IoT Device Security Capabilities" in the document, each with a brief definition, a scope, and a longer-form description under the moniker, "discussion" to capture the qualification of that capability in more narrative form. A couple of annex sections are also included that share similar capability stanzas, but without the expectation that they are part of an asserted baseline, which may evolve over future releases. Over half the document provides mapping tables to go between this document's output and many of the input standards that lead to this consensus approach. Compared to other offerings, this document is more apt to help find overlap in standards and get back to more direct guidance from influential frameworks and standards that are more detailed.

There are also industry documents released as roll-up guidance, such as "Internet of Things Security Guideline" from the IoT Alliance of Australia (IoTAA) organization (IoT Alliance Australia, 2017). Released in November 2017, this effort aggregates numerous relevant existing documents from organizations like OTA, IoTSF, OWASP, NIST, & ISO. Additional guidance is integrated from country-centric guidance (e.g., "Australian Privacy Principles"), Internet Engineering Task Force (IETF) request for comment (RFC) standards, and industry-specific guidance from the 3rd Generation Partnership Project (3GPP) as examples. In this manner, the document serves as more of a unified lens across many IoT security topics that attempts to leverage existing working group efforts, supplementally integrating additional value.

The European Union Agency for Network and Information Security (ENISA) also has its own IoT security framework approach that was released in November 2017 called the "Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures"

(European Union Agency For Network And Information Security, 2017). In the Annex A section of the document, a catalog of 83 security measures & practices are enumerated with associations to 24 categories that span technical & business focuses. Each category, rather than each individual practice, provides a detailed list of industry standards, frameworks, and guidance that influenced the final content provided. While many other such documents create referential integrity with a given piece of guidance to influential material, the ENISA publication leverages many IoT security publications instead of more generic control mappings. In this manner, the publication is somewhat of a hybrid approach between creating a unique framework and those with derivative/roll up frameworks.

CHAPTER 3

RESEARCH METHODOLOGY

In Chapter 2, the literature review provided context to anchor our study's focus on contributing real-world analysis of IoT cameras with appropriate mappings to security frameworks that inform readers of the current state of such devices across multiple dimensions of security integrity. The availability of such research today in a broad, organized, and well-curated manner is lacking, which this study sought to address with its contributions to the literature.

In this chapter, the study's research approach will be explained and justified. Details for the study's sample population, assessment-tracking mechanism, assessment environment, data collection process, instrumentation, device evidence & artifact collection, legal considerations, and limitations will also be provided.

Research Approach & Justification

A research approach helps to inform the plans and procedures that will be used to conduct a study for the researcher's selected topic (Creswell & Creswell, 2018). There are three primary research approaches to choose from – quantitative, qualitative, & mixed methods – with the ultimate choice being based on inputs, such as the researcher's philosophical assumptions, the nature of the research problem, and methods of data collection (Creswell & Creswell, 2018).

When considering the approach taken for this specific study, it is important to acknowledge that the researcher's philosophical world view was one of pragmatism. Within this philosophical worldview, researchers are free in their choices to address the study's topic in a manner that best meets its unique needs and purpose (Creswell & Creswell, 2018). With that lens

in mind, the chosen research approach for this study was quantitative, utilizing domain-specific instrumentation, data collection, techniques, and methods that can appropriately assess IoT cameras across many market segments for their multi-dimensional security integrity aspects.

A quantitative approach uses numerical, statistical, or mathematical analysis to provide results for the topic of study (Babbie, 2014). For this study, readers are presented with these types of representations for IoT camera assessment results that have been mapped to relevant security frameworks to provide analysis for their absolute and relative security achievement.

The researcher must also determine an appropriate research design within the chosen approach. One such design is survey research, which will provide a numeric description of trends for a population being studied from a sample of an overall population (Creswell & Creswell, 2018). This research design is appropriate for our topic of study as the total population of IoT cameras across the world-wide market, over multiple decades of production, are too vast to research entirely, leading to the need to present data that is representative of the total population.

Within the survey design, a cross-sectional approach was selected as it addresses a point-in-time view of the sample, rather than longitudinal, which would require data collection over time (Creswell & Creswell, 2018). To achieve data collection for this study, rigorous testing had to be conducted with instrumentation across hardware, software, cloud services, & mobile applications, which would not be feasible to conduct more than once for the selected sample size.

Lastly, this cross-sectional survey is further qualified in that it uses a descriptive-analysis approach that helps to describe and summarize data points in a way which patterns may appear from the assessed sample (Rawat, 2021). The study's focus on using IoT security frameworks to provide analysis of the raw data gathered from instrumentation means that simply providing collected data – while informative and valuable to the literature – is not by itself sufficient to

answer how such data reflects the security of IoT cameras for our chosen population sample. With this approach, the research study was able to achieve the previously stated goals.

Survey Sample Population

To assess the security of IoT cameras, a survey population must be established as the feasibility of providing robust testing for every such device available on the market is monetarily and temporally out of plausibility for such a research study to ever succeed. Further, the overall population simply has entirely too much variance in features, production dates, attack surface, and other details that make a study like this less effective to contrast security effectively.

By applying constraints to the population being assessed, a more uniform study can be achieved. Since this research study intended to address the adherence of devices to industry frameworks, choosing devices that mix eras of IoT innovation may bias certain devices towards higher rates of success, hindering the value of this study. Lastly, the study intended to look at not just one market segment, but many, helping to provide a *broad market* lens to the overall topic.

These practical constraints led to establishment of the following sample criteria:

1) A total of 40 IoT camera devices were assessed, broken into the following quantities and market segments to cover a wide range of use cases for such devices:
    a. 20 – Security cameras
    b. 5 – Baby monitors
    c. 5 – Hidden cameras
    d. 5 – Pet feeders
    e. 5 – Doorbells
2) All devices were purchased from Amazon.com, representing devices that are readily available to United States-based consumers for purchase and usage.

3) All devices were first offered on Amazon.com during 2020 to ensure they represented recent IoT devices in the market and to prevent any sample device from having a dramatic timing advantage in leveraging published IoT security guidance.
4) All devices had an approximate pre-tax purchase cost of $50 - $150 USD to control for how much a given device manufacturer may have invested in device development.
5) All devices had at least Wi-Fi connectivity and support at least one smart phone mobile application to provide consumer control over associated hardware & services.
6) The sample population avoided repeating vendors within and across assessed segments that were analyzed to increase the survey's market representation.
7) The sample population also avoided devices from different vendors that physically appeared the same to limit accidental duplication of sample devices.

Sample Size Determination

In the above criteria, it is noted that 40 total devices were chosen for the survey's sample. In practical terms, the definition of an IoT camera varies within the market and, in many cases, may come down to vendor marketing choices. The availability of a device for purchase and/or use by a researcher may be artificially constrained based on a geographic market, terms of service, legal restrictions, or otherwise. To help control for some of these variables, the use of Amazon.com was chosen by the researcher.

Even within Amazon.com, product categorization may be inconsistent. For instance, an IoT baby monitor may appear under "Smart Baby Monitors," "Video Baby Monitors," "Dome Surveillance Cameras," or many other filters. Additionally, this research intended to provide a broad-market analysis, which requires the assessment of unique vendors to bring the most comprehensive data set to the market analysis. That further limits the potential cameras that are

applicable since one vendor may offer multiple cameras for sale, eroding the total breadth of market representation across the 40 sample devices.

With all of the previously noted population constraints used to bring a healthy amount of commonality among devices sampled – while also providing enough market differentiation – finding a sufficient number of devices that could meet all of the given criteria proved to be a difficult approach due to the limitations of Amazon.com's filtering capabilities & categorization. For instance, identifying devices that were first made available in 2020 is not easily searchable and requires manual analysis of individual product pages. The availability of cameras – which was further hindered due to supply chain issues during a global pandemic at the time this research was conducted – lessened the available options which met this restrictive criterion.

This led to the less desirable, but more pragmatic approach, of this specific study being performed with a nonprobability sample, which builds the sample of the population based on convenience and availability (Creswell & Creswell, 2018). In the case of the literal Amazon.com category of "Smart Baby Monitors," for instance, 71 results are provided, but that includes vendors with more than one device, devices that were available earlier than 2020, as well as other reasons that the sample would be filtered down more than the absolute total may portray.

Finally, the reality of the study's topic is one of near-endless population. Devices produced by a single vendor may use different cloud services, firmware versions, mobile application platforms, and core software packages. These aspects are also continually evolving through feature releases and infrastructure updates. Even if a uniform population total could be determined, it would still be misleading as the variance goes far beyond a product name or model number, extending into unique instances of a device for a particular geography or release year.

In terms of appropriateness of the sample through the lens of prior literature, studies reviewed ranged in samples from five-to-ten devices (Alharbi & Aspinall, 2018; Stanislav & Beardsley, 2015), making this study's 40 devices markedly more representative. Further, and while anecdotal, the difficulty in finding enough devices that met the sample criteria is indicative that the constrained population for this study is highly representative and meets the intended needs of this study, which is to highlight devices across multiple segments through a lens of multi-dimensional security integrity. This sample achieved the stated goals for this study's focus.

Table 1 provides the list of the IoT cameras that were selected for this study's sample, including details such as their model, price, FCC ID, and relevant market segment.

Table 1. *Research survey sample device listing.*

Brand	Model	Price	FCC ID	Market Segment
Akaso	CS300	$48.99	Not Found	Security Camera
Amcrest	ASH42	$50.99	ZZ2-Z10	Security Camera
Anbes	BF-A10	$49.98	2AR5E-BF-A10	Security Camera
Anran	AR-W620	$56.69	2AZUX-S02	Security Camera
Aqara	CH-H01	$69.99	2AKIT-G2H	Security Camera
Camakt	WiFi Picture Photo Frame	$56.99	Not Found	Hidden Camera
CellBee	SC-AI04	$102.73	2AS4ASCAI01	Baby Monitor
Conico	ZS-GX3S	$55.99	2AT5D-ZS-GX5	Security Camera
DCT	CG1	$63.99	2AXBN-CG1	Security Camera
Didog	FDB073-T980USA	$111.99	Not Found	Pet Feeder
Ecobee	EBSCV01	$99.99	WR974100118120	Security Camera
Ecwey	EV200	$51.29	Not Found	Hidden Camera
Energizer	EOD1-1002-SIL	$49.99	2AG7C-BELL5S	Doorbell
Euarne	K-BELL 1c	$47.69	Not Found	Doorbell
Eufy	T8222	$129.99	2AOKB-TB220	Doorbell
Eversecu	Outdoor Wireless Camera	$56.99	Not Found	Security Camera

Brand	Model	Price	FCC ID	Market Segment
Feit Electric	CAM/PAN/WIFI	$51.21	SYW-CAMPANWIFI	Security Camera
HeimVision	Protect D1	$55.99	2AWRR-PRD	Security Camera
HONGSA	Automatic Pet Feeder	$99.99	Not Found	Pet Feeder
IOIODOG	Pet Auto Feeder	$123.49	Not Found	Pet Feeder
iSmartPet	97089	$119.95	Not Found	Pet Feeder
Jennov	A90WT20-1-FAS-32	$65.50	Not Found	Security Camera
Kami Baby	Kami Baby Monitor	$99.99	2AFIB-YYS5019	Baby Monitor
LaView	LV-PWR12W	$49.99	2APD7-R9820	Security Camera
Mascarry	A4	$50.99	2AUAU-A4	Security Camera
Moonxiao	Robot	$56.99	Not Found	Security Camera
Motorola	Connect40	$129.99	VLJ-CF85BU	Baby Monitor
Pambrum	spy cam clock-208	$55.99	Not Found	Hidden Camera
Reolink	Lumus	$49.99	2A7V-1909A	Security Camera
Sekoya	PP003	$129.99	2AXFT-PP003	Pet Feeder
Sense-U	SU-WA002	$129.99	Not Found	Baby Monitor
StartVision	L-18	$65.99	Not Found	Security Camera
Swept Supplies	Ninja Pro Hidden Camera	$84.99	Not Found	Hidden Camera
TP-Link	EC70	$49.99	TE7KC115	Security Camera
Vacos	Vacos Cam	$99.99	2AKL2K44IPC	Security Camera
Victure	VD300	$54.99	2AREL-VD300	Doorbell
VicZone	Y13	$94.99	Not Found	Hidden Camera
VTech	VM901	$139.95	EW780-1957-00	Baby Monitor
WOHOME	LY-138	$53.99	2AFCB-LY138	Security Camera
Wuuk	W0001	$89.00	2AWHY-W0001	Doorbell

Creation of a Custom Assessment-tracking Mechanism

A custom assessment-tracking mechanism was created so that individual security properties could be cataloged for each sampled device in a detailed and uniform manner. The composition of this tracking mechanism was influenced by currently available IoT security frameworks by extracting their criteria in a manner that created a robust and deduped view of assessment data that could then be mapped against many forms of published guidance.

The chosen frameworks to analyze for this tracking mechanism were OWASP's ISVS v1.0RC (Guzman & Bassem, 2021), CSA's "IoT Controls Framework" version 2 (Cloud Security Alliance, 2021), and IoTSF's "IoT Security Compliance Framework" version 2.1 (IoT Security Foundation, 2020). These choices were made to provide representation for different types of technical organizations, the years guidance was released, and breadth of controls – 933 in total – along with broad coverage of security topics represented across those controls.

Once determined, each framework's controls were imported into a unified spreadsheet that allowed for designating whether a given control was in scope for this research agenda or not. A control was excluded from consideration if there was no way to test for it during the research. This was common when the framework's control described an internal business process that was unable to be tested for using only the research devices. The results of this exercise can be seen in Table 2. Other controls may have been excluded when the merit of the control was not relevant to security or privacy considerations and therefore not applicable to the study's goals.

Table 2. *Framework control scoping for assessment-tracking mechanism inclusion.*

Framework	Controls In-scope	Controls Out-of-scope	Total Controls	% In-scope
OWASP	102	22	124	82%
IoTSF	139	100	239	58%
CSA	63	92	155	41%
Total	304	214	518	59%

Once these controls were aggregated, a mapping was performed that defined each control in a one-to-many association to 12 different technical security categories that themselves were derived by de-duplicating and normalizing category/grouping types used in the frameworks. Figure 1 provides a visualization of the category distribution from this process. The purpose of this step was to ensure that there was reasonable representation across numerous different types of security categories to identify gaps more easily in the meta data that the assessment-tracking mechanism would ultimately attempt to uniformly index for later analysis.

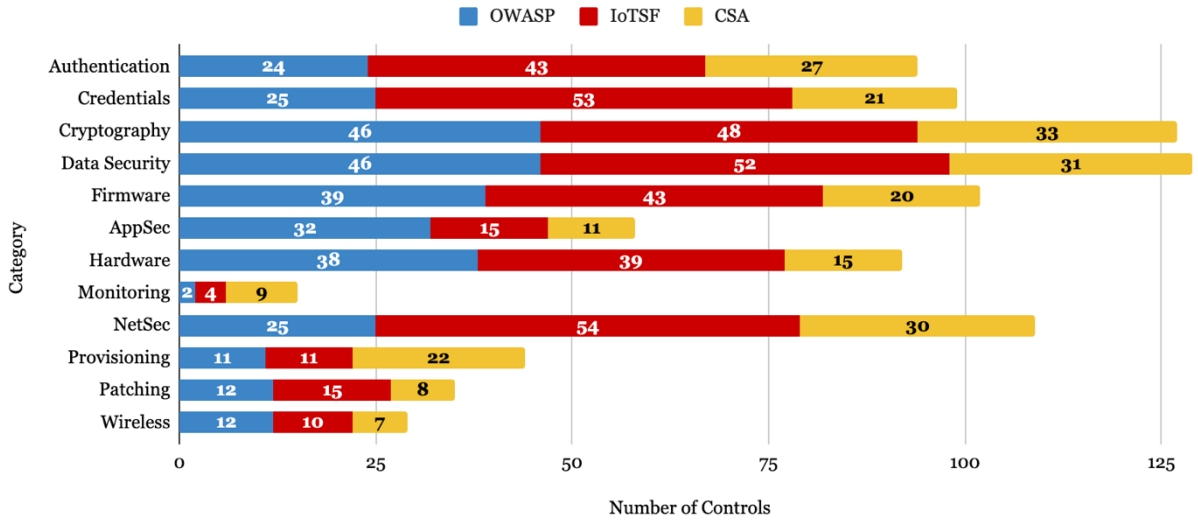

Figure 1. *Security control-to-categorization mapping totals.*

After scoping and category-refinement occurred, the next step was to generate a set of assessment goals that would provide data that would help to answer the overarching intention behind controls that were gathered. In practice, frameworks often overlap security goals redundantly, whether directly or with similar wording that does not materially change the focus. With our initial 518 controls, this approach was able to reduce the assessment complexity down to 68 assessment goals with evidence criteria associated to it. This served as the basis of the meta data that would ultimately provide a uniform approach to what data was needed to capture, the

types of sources that may provide that data, and the tooling that might be required for analysis. A table that represents these 68 assessments goals including a description, evidence focus, and the number of unique controls across the three referenced frameworks can be found in Appendix I.

The final step of building the custom assessment-tracking mechanism was converting assessment goals into discrete columns that would track desired meta data or testing outcomes in a manner that would allow for easily mapping the results against frameworks after analysis of the sample was finished. This structure also captured higher-level data about the sample, such as the device's vendor, serial number, mobile applications details, etc. that were not necessarily for using in control mapping analysis, but rather descriptive of the device for useful reference.

The resulting data structure was built in a spreadsheet, allowing for easy numerical analysis and chart generation from the data set. While a relational database or similar storage mechanism could have also been used, the flat nature of the data and lack of need to conduct complex queries negated the value of that additional overhead. The data could be easily imported from CSV (or similar) into a database for future research if deemed necessary.

The resulting spreadsheet contained 160 total columns organized into logical sections for easier reference (e.g., Wi-Fi, Firmware Updates). During the analysis of each device in the sample, data was populated into all relevant columns. When data was simply unable to be found, an *Unknown* reference was denoted. In cases where data was irrelevant due to the device's feature set, an *N/A* was used. All other data populated was done so via testing outcomes.

The multi-step process taken to generate the resultant custom assessment-tracking mechanism was done to obviate bias by determining the data to gathering from a variety of IoT security frameworks that represented recent industry guidance within their controls. Because the goal of this research agenda was to map sample device findings to frameworks and provide a

representative data sample that could be used by other researchers, this approach provides insights that are able to be applied to many IoT frameworks, rather than only address the outcomes as mapped in a one-to-one fashion.

Assessment Environment

In Figure 2, a logical diagram provides a high-level association of the study's testing environment. Each of the sample devices were tested with a combination of three assessment devices representing macOS, Linux, and Android-based operating systems, providing robust instrumentation as defined throughout the remainder of this section. The assessment required conducting analysis of not only the physical IoT device, but also relevant cloud services and mobile applications provided by vendors. The variability of a given IoT device's ecosystem required a mixture of technical approaches to achieve data collection goals for this study.

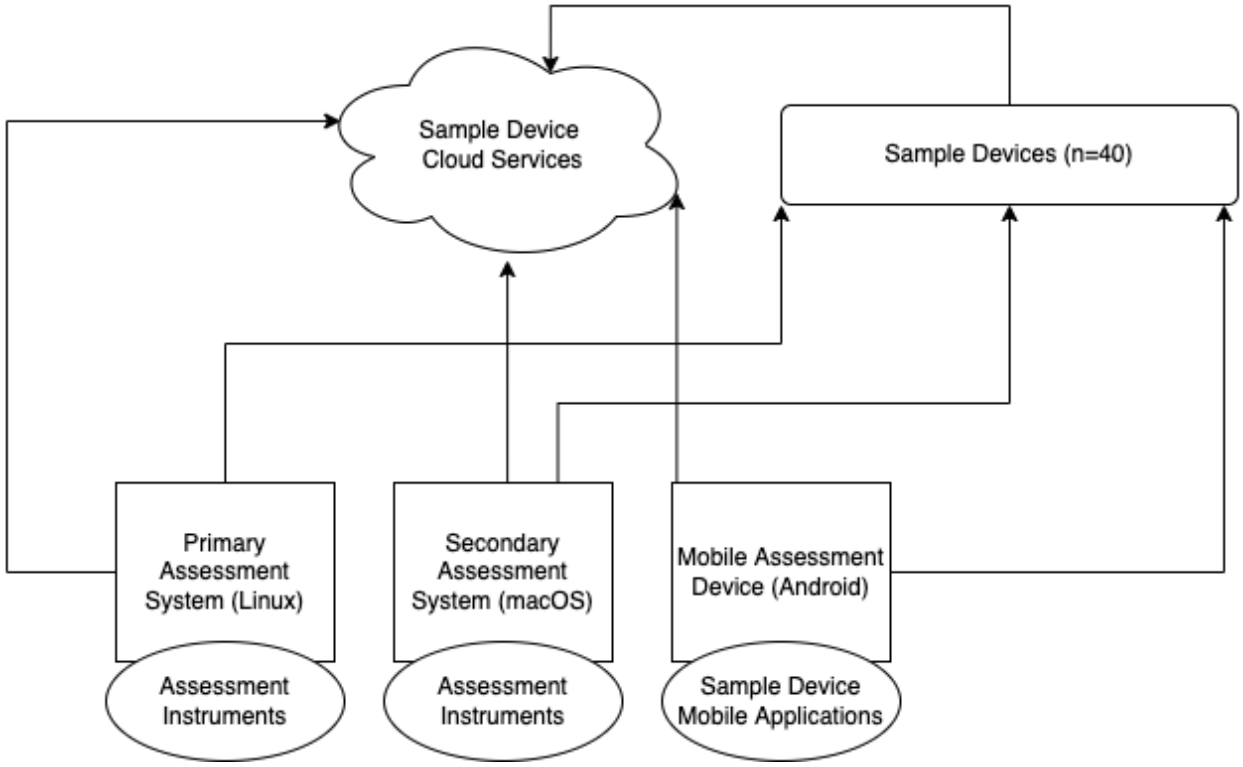

Figure 2. *Assessment environment diagram.*

The evaluation process occurred in a home-lab environment with a static set of testing systems and tooling – briefly described below – to ensure continuity between assessed samples.

Primary Assessment System

- **Hardware:** Raspberry Pi 4 Model B
- **Operating System:** Kali Linux (2020.2 - 2021.4)

Secondary Assessment System

- **Hardware:** Apple MacBook Air (Mid 2013)
- **Operating System:** macOS (11.3.0 - 11.6.1)

Mobile Assessment Device

- **Hardware:** Motorola Moto G7 Play
- **Operating System:** Resurrection Remix 8.6.4 (Android 10)

Assessment Wi-Fi Access Point

- **Hardware:** TP-Link WR841N
- **Operating System:** DD-WRT (tl-wr841ndv8)

Additional Assessment Hardware

- Multimeter
- USB to TTL serial cable
- Soldering iron
- Hot air gun
- eMMC breakout socket
- Soldering station
- Shikra
- Bus Pirate
- SOIC 8-pin clip
- Magnifying glass

Core Assessment Software

- **Mobile Man-in-the-Middle:** *mitmproxy*
- **Network Packet Capture:** Wireshark
- **ARP Spoofing:** *bettercap*
- **Extract APK:** *d2j-dex2jar* & *apktool*
- **File Analysis:** *file*, *grep*, *hexdump*
- **USB Listing:** *lsusb*
- **Password Cracking:** *hashcat*
- **Binary Security:** *checksec*
- **SSL/TLS Security:** *sslyze* & *sslscan*
- **Wi-Fi Analysis:** *kismet*
- **Serial Console:** GTKterm
- **Firmware Analysis:** *binwalk*
- **Flash Dump:** *flashrom*
- **Port Scanning:** *nmap*
- **Android Debug:** *adb*
- **RTSP Streaming:** VLC & *ffmpeg*
- **MQTT Analysis:** MQTT Explorer
- **Binary Analysis:** IDA & Ghidra

Data Collection Process

The following overview represents a common case analysis of a given device in the sample. Due to the heterogeneous nature of IoT devices and their relevant ecosystems, there is no simple, one-size-fits-all approach to analysis. There are, however, many typical steps and goals that were followed that will help to highlight a general approach to the evidence gathering and analysis that led to the resulting data found in Appendix G.

The variability of any step noted depends greatly on the specific hardware configuration, operating system, security controls, device settings, and other aspects that can only be known once a sample device is interacted with. This leads to gaps in assessment data in some cases or just a lack of applicability to assessment criteria in other cases.

In the case of dumping a flash chip, for instance, an 8-pin SOIC clip may allow for easy access to those contents using *flashrom*. In some cases, however, the flash chip is unlikely to dump cleanly without removing certain leads to the printed circuit board. This may require that a flash dump occurs with a "chip off" approach, where the chip is de-soldered from the device and then attempted to be dumped. In other cases, the flash may not have easily exposed leads, such as an eMMC flash chip. This will also require a chip off so the flash can be placed in a special socket that then connects to an assessment computer via an SD card slot to read its contents.

When an operating system (OS) or bootloader can be interacted with directly, greater accuracy can be gleaned. In some cases, the lack of a running environment prevents asserting a conclusion due to the need to see how configuration has been applied that may appear one way inside of a file but is modified during operation. Many cases arose that required the use of an *Unknown* designation to be applied for data in the assessment-tracking mechanism due to this.

Phase 1 – Device Information & Artifacts

1. Document general information about each device (e.g., vendor, model, UPC, price, etc.)
2. Take photos of the device's packaging and the exterior of the device (e.g., shell, ports)
3. Document and archive copies of the device's Amazon.com and vendor product pages
4. Determine if the device's vendor has published contact details for security issues
5. Locate an FCC entry for the device, if applicable, and archive posted device photos
6. Document any packaging or user-manual claims by the vendor about device security

Phase 2 – Internal Device Analysis

7. Open the device's exterior shell, documenting core chipsets with photos and data sheets
8. Determine if there are any tamper-evident controls in place for external or internal access
9. Review data sheets for each chipset and document relevant features (e.g., Secureboot)
10. Attempt to dump available SOIC flash memory packages without removing the chip
11. If a flash dump was achieved, attempting to identify and/or crack passwords
12. If a flash dump was achieved, determine if the filesystem is encrypted and its format
13. Identify candidate UART interfaces (e.g., silkscreen markings, multi-meter readings)

Phase 3 – Mobile Application Information & Artifacts

14. Identify the device's mobile application and inventory details (e.g., release date, version)
15. Download the mobile application's APK and extract source code & meta data from it
16. Determine if the mobile application is using a Tuya-based framework for its functionality
17. With man-in-the-middle enabled, open the device's mobile application for initial usage
18. Determine if the mobile application warns the end-user that a "rooted" device is in use
19. If applicable, attempt to register for the cloud service with the mobile application
20. If able to register, document the password policy and two-step verification configuration
21. Interact with the mobile application, taking screenshots and recording packet captures
22. Determine if API calls fail, even with attempted man-in-the-middle functionality enabled
23. Determine if the device utilizes a specific identifier for the device when sending requests
24. Determine if the device has any default credentials that allow authentication into it
25. From mobile application packet captures, determine if all HTTP APIs are encrypted

26. Analyze the mobile device's filesystem to determine if sensitive data is in cleartext
27. Document time synchronization provided by the mobile application's configuration

Phase 4 – Network Interface Configuration

28. Determine if Wi-Fi setup allows for WPS, QR code, and/or temporary network pairing
29. If temporary network pairing is used for Wi-Fi setup, determine if a password is required
30. Document the Wi-Fi MAC address of the interface from the device being assessed
31. Determine if the device supports 2.4Ghz and/or 5Ghz radios for its operation
32. Determine if the device supports the WPA3 protocol for Wi-Fi communication
33. Determine if Bluetooth configuration is used, and if so, what protocol version is used
34. If Bluetooth configuration is not automatic, document the pairing approach used
35. If the device provides Ethernet-based connectivity, document its MAC address
36. Document if the device provides any sort of Zigbee support (e.g., hub or client) modes

Phase 5 – Access the Running Device

37. Connect to available USB interfaces to determine any debug and/or mass storage features
38. Assess candidate UART interfaces to determine their baud rate, pin out, and use case
39. Identify the running bootloader and operating system if SoC UART access was gained
40. Document any identified bootloader and/or OS output that is sent to the serial console
41. Assess from boot messages if Secureboot and/or cryptographic kernel verification is done
42. Determine if any sensitive data/secrets are exposed in serial console output via UART
43. Attempt to access the bootloader, running further analysis commands if successful
44. Attempt to login to the OS, if applicable, with common or recently found credentials

Phase 6 – Network Service Analysis

45. From network packet captures, determine if MQTT is used during the device's operation
46. If MQTT is used, document its operating port and whether it uses transport encryption
47. Determine if sensitive data shows via any UART serial consoles after device setup
48. When the device is on the test network, run and archive a full TCP port scan of its IP

49. Discover any FTP, Telnet, SSH, and/or RTSP services exposed on the local LAN
50. If RTSP is available, document its port, transport security, and if it uses authentication
51. If a web server is found, document its banner and port information as identified
52. If a web server is found, document if it is over cleartext or using SSL/TLS for transport
53. If a web server is found and using SSL/TLS for transport, archive a security scan score
54. If a web server is found, document if its services require any form of authentication
55. If a web server is found, does it limit any authenticated sessions in the duration of use
56. If a web server is found, and requires authentication, document any brute-force protection

Phase 7 – Firmware Upgrade Analysis

57. Determine if a firmware upgrade feature is supported for the end-user to access
58. Determine if the device requires that the latest firmware upgrade is installed before use
59. Determine if the mobile application informs users of an available firmware upgrade
60. Determine if the mobile application allows users to check for new firmware upgrades
61. Determine if users can manually install firmware images with a supported workflow
62. Attempt to acquire packet captures for the firmware upgrade process and archive those
63. If firmware upgrades are intercepted, determine if the upgrade uses transport encryption
64. If firmware upgrades are intercepted, determine if the upgrade file is encrypted at rest
65. If firmware upgrades are intercepted, determine if the download requires authentication
66. If firmware upgrades are over an encrypted transport, determine the SSL Labs score for it
67. Determine if cryptographic hashes and/or signatures are used for firmware verification
68. If firmware was upgraded, perform another flash dump to have a new firmware dump

Phase 8 – Linux-based OS Analysis

69. If Linux root access has not been achieved, try to use single-user mode via the bootloader
70. If Linux root access has been achieved, backup the filesystem to an SD card if able
71. Determine if any form of malware detection software is running on the device
72. Document any accounts that are found and any associated cryptographic password hash
73. Document the Linux distribution, the distribution's version, kernel version, and build date
74. Identify if core kernel modules have been cryptographically signed as installed

75. Determine if any container-based technology (e.g., docker) is in use for running services
76. Select a binary that represents a core system service that is vendor-specific, not generic
77. Determine if RELRO, stack canaries, NX, PIE, and/or Fortify are used on that binary
78. Determine if debugging symbols have been removed from that binary
79. Determine any IMA, watchdog, cgroup, KASLR, ASLR and/or seccomp-bpf usage
80. Document all running processes and all listening network ports & sockets
81. Determine if most services are running as root or using less-privileged accounts
82. Determine if any mandatory access control technology is available and in use
83. Determine if filesystem discretionary access controls are appropriately configured
84. Determine if IP traffic forwarding between network interfaces is enabled
85. Determine if a host-based firewall is used to provide network access control

Phase 9 – Privacy Analysis

86. Document if an LED illuminates when the camera is streaming video with any method
87. If an SD card is supported, determine the filesystem used and if data is unencrypted
88. If supported, attempt a factory reset of the device using the documented physical reset
89. If a factory reset occurs, review any SD card for camera recordings that are still present
90. If a factory reset occurs, perform another flash dump to have a new firmware dump
91. If a factory reset firmware dump is achieved, review it for sensitive strings still present

Phase 10 – Data Completeness & Quality Check

92. Identify any gaps in artifact collection and follow the relevant assessment process steps
93. Review collected artifacts to populate missing data in the assessment-tracking mechanism
94. Verify that assessment-tracking data was populated without input errors or format issues

Instrumentation Details

Table 3 and 4 identify several of the common – but not exclusive – commands that would be ran for various operations to gather data from the research sample. Additionally, the context of that command and its general purpose are noted as part of this overview. This information helps to explain the types of approaches that further researchers may use themselves.

Table 3. *Assessment-device instrumentation command list.*

Command	Description
checksec --file=[file]	Provide binary hardening results for a file
adb devices -l	List all connected Android devices via USB
lsusb -v -t	List all connected USB devices
flashrom -p buspirate_spi:dev=/dev/ttyUSB0 -r [file]	Read the contents of a flash chip into a file
d2j-dex2jar [file]	Interpret an APK into Java class files
nmap --script banner -sT -p1-65535 -A -T4 -sV [IP]	Scan an IP's TCP ports with extra metadata
binwalk -Mre [file]	Extract known files recursively from a file
ffmpeg -i rtsp://[IP]:554 -ss 0 [file]	Record an RTSP stream from an IP to file

Table 4. *On-sample (Linux) instrumentation command list.*

Command	Description
ps w	List all processes and expanded arguments
sestatus	Provide the status of SELinux settings
netstat -nlp	Provide listening network ports with a PID
cat /proc/sys/net/ipv4/ip_forward	Check for IP traffic forwarding usage
cat /proc/cpuinfo	Show CPU metadata, including feature sets
cd /usr/modules/; for i in `ls`; do grep sig $i; done	Find evidence of signed kernel modules
cat /proc/sys/kernel/randomize_va_space	Determine the running ASLR configuration
iptables -n -L -v	Determine the firewall configuration
ifconfig -a	List all available network interfaces
cat /etc/passwd /etc/shadow	Show system accounts & password hashes

Device Evidence & Artifact Collection

For each assessed device, the following folder structure was used on a per-device basis to track & organize files that were gathered from instruments and other approaches:

- **Documentation:** Hardware data sheets, web page screenshots, and digital user manuals
- **Evidence:** Packet captures, port-scan results, serial output, and TLS-scan screenshots
- **Firmware:** Flash dump files, filesystem copies, and vendor-provided firmware images
- **Mobile App:** The APK, extracted data from *dex2jar*, and extracted data from *apktool*
    - **Screenshots:** Captured screenshots that were taken for mobile application views
- **Photos:**
    - **External:** Photos of multiple angles of the device's exterior and available ports
    - **FCC:** Exports of internal and/or external photos by the vendor for FCC review
    - **Internal:** Photos of multiple angles of the device's interior chipsets and boards
    - **Packaging:** Photos of the device's packaging, especially for labels and markings

Additional screenshots may have been taken for devices, such as when a device features an undocumented web service with administrative configuration capabilities. Serial console output was often captured in multiple files, usually to track the kind of output that was being observed (e.g., bootloader output, OS kernel messages, command output) more uniformly for future review. An attempt was made to capture most outputs that would provide for a direct piece of evidence for results within the assessment-tracking mechanism. However, in some circumstances, this data was either implicit (e.g., not supported) or identified in a manner that required active analysis (e.g., firmware extraction) such that the finding is less obvious in data.

The reality of firmware upgrades, cloud service changes, mobile application updates, and similar elements precludes asserting any finding that was not within a device's testing window.

Legal Considerations

The research agenda was conducted utilizing IoT cameras that were acquired by the researcher for the distinct purpose of this academic study. To avoid any accidental access of another consumer's data, each device was be purchased new-in-box directly from Amazon.com and all assessments were limited to user accounts and data generated by the researcher. A dedicated e-mail account was registered that represented the author's real name and was exclusively used for testing purposes when cloud services were part of the device's ecosystem.

Further, all assessment activities were conducted in alignment to the U.S. Copyright Office's definition of "good-faith security research" as described in their security researcher exemption of the Digital Millennium Copyright Act (DMCA) for research conducted against consumer devices (U.S. Copyright Office, 2015).

Data Collection Limitations

The variance in sample device composition for this topic of study implicitly limited the researcher's ability to control observability for all data intended to be gathered within the assessment-tracking mechanism. Sample devices, while uniform in constraints applied for population criteria, vary wildly in their vendor's implementation of hardware selection, operating system usage, software development, mobile application feature set, cloud service usage, and otherwise. This reality is managed by marking findings for each device in the sample with an affirmative result from instrumentation (e.g., a measurement), an *N/A* for data that is simply not relevant to the vendor's approach for their device, or an *Unknown*, if the data may be present, but is undiscoverable – for a variety of reasons – during the research timeline.

The sample of this population are made of technologies, not people, with results for the survey having been derived from instrumentation based on device-specific features and functionality. Attempts, in some cases, to limit a researcher's ability to observe a given technology as part of the device design can intentionally hinder such analysis, restricting the depth a sample may provide relative to others from the population sample. These devices are not intentional *participants* within this study, thereby limiting the pre-ordained applicability that could be determined prior to the purchase and direct analysis of the sample for its inclusion.

CHAPTER 4

RESULTS

The purpose of this research was to gather security attributes of modern IoT camera devices and then map those against industry frameworks to provide a method for determining the security of sample devices in a way that can be compared to one another uniformly and broadly. Chapter 4 provides the results from mapping the gathered data set against three IoT security frameworks to show quantitative trends and provide for key insights from the analysis.

Overview

The research conducted for this study has provided device-specific findings across the survey sample (n=40) to allow conclusions about the security of modern internet-connected cameras representing five different market segments to be drawn. All results are presented as their unweighted values; thus, interpretation of raw outcomes will not account for variance in the potential security-value of a control. This should be kept in mind during the analysis of findings presented within the results and conclusions of this dissertation. The security of sample devices were assessed by mapping data against three IoT security frameworks:

1. DCMS "Code of Practice for Consumer IoT Security" (U.K. Department for Digital, Culture, Media & Sport, 2018)
2. ETSI "Cyber Security for Consumer Internet of Things: Baseline Requirements," EN 303 645 V2.1.1 (European Telecommunications Standards Institute, 2020)
3. A proposed IoT security framework (see Appendix A) generated as a contribution to the literature as part of this dissertation (herein referred to as "proposed framework")

Of specific note, the ETSI guidance was influenced – as per its own in-document notice – by the DCMS guidance, especially as it relates to the categorization used. Because of this, there are nearly identical naming conventions for the category breakdown. However, DCMS provided generalized framing in a short paragraph per focus area, while ETSI has much more depth. In practice, the mapping of study results to these frameworks will have overlap in some places but diverge in many others. Whereas DCMS had nine high-level topics receive a mapping for this study, there were 42 more-granular mappings that occurred for the ETSI guidance.

Proposed IoT Security Framework

During both this dissertation's literature review and the initial analysis of the survey sample's results, it was noted that there existed an opportunity for a different lens to be created and applied during the analysis phase of this study. While the literature review makes a strong case that the industry is not lacking perspectives on IoT security in terms of variety, the approaches taken by the represented organizations may still leave room for another entry into the mix. Technical frameworks for any industry will always have aspects that are more-or-less applicable to given targets, which was made apparent during this research study.

Existing IoT security frameworks range between extremely granular, such as IoTSF's 240 controls (IoTSF, 2020) and extremely terse, such as DCMS' 13 controls (U.K. Department for Digital, Culture, Media & Sport, 2018). Highly granular frameworks can make it difficult to focus in on what meaningful security looks like, versus all the possible improvements that could be made. While more security controls may sound helpful, the variability of impact makes it so that a lot of effort could be wasted on controls that do very little for the practical security risks of a device like a consumer camera. Very terse frameworks, however, can create a lot of ambiguity in terms of what the successful implementation of a security principle looks like.

When a framework associates assessment guidance with a given control, the language of that guidance may conflate numerous criteria into one testing approach, making it difficult to tease apart the actual *success* of that control in practice. It is reasonable that a control may have various ways to achieve that guidance, but the sometimes-prescriptive nature of the approach can hinder assessment across the vastly heterogenous devices that IoT market segments represent. If test guidance is too layered in criteria, an assessor – especially within an internal product security team – may bias their conclusions of control compliance for facets they focused on and ignore other aspects that they find less important. When it is difficult to draw a straightforward *success* or *failure* conclusion for a test, implicit bias could more easily set in.

Lastly, when frameworks are created, their authorship will always have a bias in the types of controls that are added relative to their organization's interests, domain expertise, and/or the industry that the guidance is being written for. That approach is meaningful when devices are built towards guidance that matches up well, but in many cases, there may be unapplied controls or entirely missing topics in assessment criteria. This leads to inconsistent result sets that make it hard to compare samples across market segments to one another.

The proposed framework (see Appendix A) was created without an intention to solve for the perhaps intractable issues of creating a perfect IoT security framework for every market, but rather to provide a more uniformly applicable framework that allows analysis of this research study's data set. There are a few major elements to the approach taken in generating this proposed framework that are worth noting to speak to how it strives to achieve that outcome:

1. A total of 66 controls are associated to ten control groupings providing a reasonable amount of both breadth and depth, without trying to "boil the ocean" of possibilities

2. Control groupings attempt to cover areas that are sometimes overlooked for an IoT device's ecosystem, such as mobile companion applications and cloud services
3. Focus was placed on controls that more directly speak to – in their relative categories – aspects of meaningful security that provides for actual risk mitigation in practice
4. Controls were generated by "reverse engineering" the data structure of the assessment-tracking mechanism, allowing for a high-degree of uniform applicability of the device samples; especially those using Linux-based operating systems
5. Wording for control descriptions was kept extremely simple so that the merit of the control was made as clear as possible, without being ambiguous to the intention
6. Wording for control test criteria was also kept extremely clear to limit the number of layers that need evaluation to draw a conclusion of the test's intended outcome
7. One-identifier dependency mapping is also provided so that someone testing for controls can more easily understand when controls may become out-of-scope
8. The simplicity of controls and their associated tests means that it is easier to determine that a control is not applicable to the sample device or that insufficient data is available, resulting in an *unknown* conclusion, rather than assuming an outcome

Some of the controls within the framework also are highly-specialized to a camera-based IoT device, such as whether an LED is illuminated when someone is viewing the camera's stream for a privacy consideration. This is a salient example that while the framework may have a great deal of applicability for this research study's survey sample, it will not likely be valuable to someone analyzing IoT leak sensors, for instance. As with any framework, understanding the intended applicability is the first step to deriving value from its insights.

Proposed Framework Results

When interpreting the following findings, a *Pass* will represent a control that was shown to meet the intent of all test criteria, a *Fail* will represent a control that was shown to not meet the merit of test criteria, an *Unknown* means that insufficient data was available to evaluate the test criteria, and an *N/A* means that the specific control was either irrelevant to the sample device's composition or excluded due to a dependent control already being a *Fail*.

The results in this section will refer to "absolute testing numbers," which reflect percentages derived from a control outcome against the total number of controls (66) for the proposed framework. Additionally, the results will also make note of "affirmatively tested controls," which refer to a percentage derived against that device's total of *Pass* and *Fail* results combined. The latter is valuable because it helps to provide a value that reflects more about what was able to be tested that the absolute number cannot provide as uniformly.

When not noted explicitly, absolute testing numbers are being reflected in percentages contained within the proposed framework results provided. Affirmatively tested numbers will be represented explicitly to disambiguate how the math highlighted was derived in calculations.

Additional data for these results, including the inputs that yield represented percentages of control outcomes, may be found in Appendix B of this document.

Overall Market Segment Analysis

Reviewing market segment data across the survey sample (n=40) by the proposed frame (shown in Table 5) allows us to conclude that Hidden Cameras (n=5) had the lowest rate of achieved compliance with 24.2% overall and 32.3% across affirmatively tested controls. Only in absolute failure numbers did Hidden Cameras perform slightly better than Pet Feeders (n=5) with 50.9% compared to 53.6%, respectively. Pet Feeders also performed poorly overall with a 29.1%

absolute pass rate and 35.2% for affirmative testing. These are both many percentage points lower than their respective overall averages across totals.

Table 5. *Proposed framework - market segment control outcome summary.*

Market Segment	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Baby Monitors	38.5%	46.1%	13.3%	2.1%	45.5%	54.5%
Doorbells	37.6%	33.3%	22.7%	6.4%	53.0%	47.0%
Hidden Cameras	24.2%	50.9%	15.8%	9.1%	32.3%	67.7%
Pet Feeders	29.1%	53.6%	13.0%	4.2%	35.2%	64.8%
Security Cameras	34.9%	38.4%	19.6%	7.0%	47.6%	52.4%
Average	32.9%	44.5%	16.9%	5.8%	44.4%	55.6%

In positive security compliance, Baby Monitors (n=5) had the most favorable absolute pass rate but only the third-strongest result when viewed with affirmative testing ratios. Through that perspective, Doorbells (n=5) performed the best at 53% and came in a close second in absolute terms with a 37.6% compared to Baby Monitors being less than a percentage point higher. Doorbells had a much better rate of avoiding failure conditions with only 33.3% in absolute numbers and a 47% rate from affirmative test results. Compare this to Baby Monitors with 46.1% and 54.5%, respectively, and it becomes apparent that Doorbells were a much stronger segment in general.

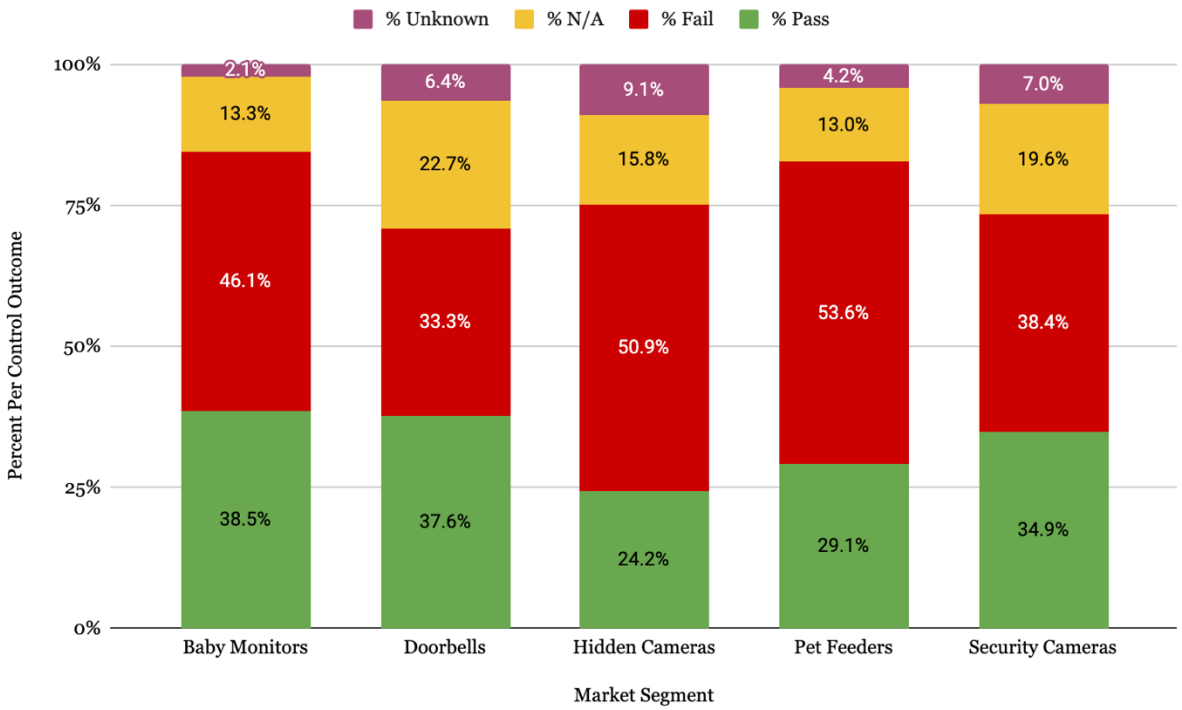

Figure 3. *Proposed framework - control outcomes by market segment.*

Figure 3 highlights that in aggregate, Doorbells not only had the most compliance to the proposed framework controls, but also had the lowest absolute and affirmative testing ratios when it came to failure cases, with 33.3% and 47%, respectively. While the absolute numbers may be biased by the fact that it had the highest rate of not-applicable controls at 22.7%, the affirmative testing ratio helps to note that among the controls that were tested, the outcome as noted prior was still the best one.

The largest assessed segment, Security Cameras (n=20), had ratio outcomes across absolute and affirmative testing approaches that favorably beat the overall averages calculated across segments. In absolute testing numbers these devices had the lowest failure rate with 38.4%, which is much lower than the overall average of 44.5%. Considering the sample size influence those cameras had on the average, this is even more impressive in absolute terms.

Individual Market-segment Analysis

Baby Monitors

Within the Baby Monitor market segment (n=5), the Sense-U camera had the lowest pass rates and highest failure rates, even when assessed across absolute and affirmative testing ratios. For instance, the absolute pass ratio of Sense-U was 24.2% which was nearly 9% worse than CellBee (33.3%) and its affirmative pass ratio was 31.4%, nearly 6% lower than CellBee. That comparison may be favorable, until you note that CellBee was still over 10%-points lower in absolute pass ratio than the next closest rate with Motorola at 43.9%. In general, Sense-U was clearly the least performant of the market segment survey, with CellBee coming next.

Table 6. *Proposed framework - baby monitor control outcome summary.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
CellBee	33.3%	56.1%	10.6%	0.0%	37.3%	62.7%
Kami Baby	45.5%	39.4%	12.1%	3.0%	53.6%	46.4%
Motorola	43.9%	42.4%	9.1%	4.5%	50.9%	49.1%
Sense-U	24.2%	53.0%	21.2%	1.5%	31.4%	68.6%
VTech	45.5%	39.4%	13.6%	1.5%	53.6%	46.4%
Average	38.5%	46.1%	13.3%	2.1%	45.5%	54.5%

For positive segment outcomes, Kami Baby, Motorola, and VTech all had approximately the same results within a few percentage points in any given comparison as seen in Table 6. We can observe that Kami Baby and VTech had the exact same pass (45.5%) and fail (39.4%) outcomes, with only minor variance for other outcomes. That same ratio alignment is also then seen for affirmative testing. Still, these cameras only performed slightly better than Motorola, so

in practical analysis – and considering variance in not-applicable and unknown outcomes – there's effectively a tie across these three survey sample devices.

The results displayed in Figure 4 help to show the tight result-set of the three higher-performing baby monitors more clearly, as well as making the less performant offerings stand out for their lower pass rates and higher failure rates in absolute.

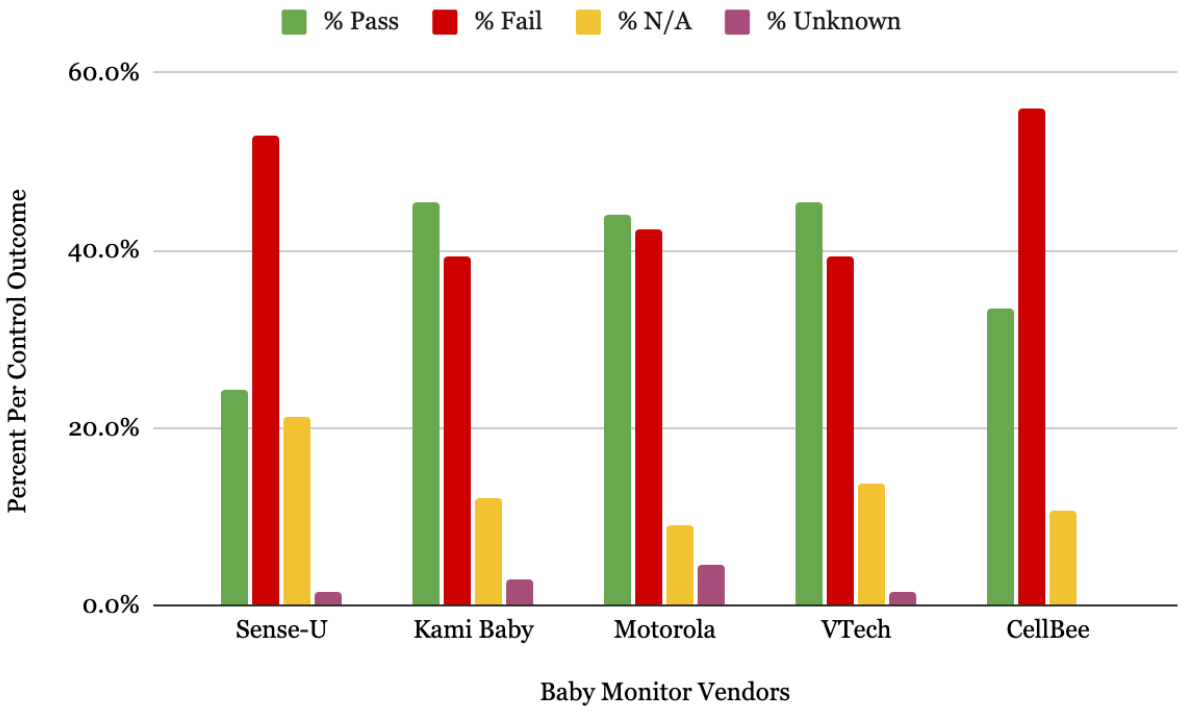

Figure 4. *Proposed framework - control outcomes for baby monitors by vendor.*

Doorbells

The Doorbell market segment (n=5), as noted in our broader segment-based analysis above, represented the overall most favorable results for comparisons as seen in Table 7. Through affirmative testing we can see that Wuuk had a pass rate of 40.4% – well below the 53% average – and a failure rate of 59.6%, which is also high above the 47% average. This

camera also was tied for the second-worst absolute pass rate at 34.8% with Victure and had the highest absolute failure rate at 51.5% -- more than 10%-points higher than the next worst result.

If we more appropriately compare Wuuk's result to Energizer, due to similarity in not-applicable control ratios, we can see that while neither had desirable failure rates overall, Energizer had the highest absolute pass rate of all devices. This helps clarify that in segment-level comparison against a device with relatively similar scopes of affirmatively tested controls, Wuuk is the clearest sample with negative outcomes.

Table 7. *Proposed framework - doorbell control outcome summary.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Energizer	48.5%	40.9%	4.5%	6.1%	54.2%	45.8%
Euarne	30.3%	24.2%	36.4%	9.1%	55.6%	44.4%
Eufy	39.4%	24.2%	33.3%	3.0%	61.9%	38.1%
Victure	34.8%	25.8%	30.3%	9.1%	57.5%	42.5%
Wuuk	34.8%	51.5%	9.1%	4.5%	40.4%	59.6%
Average	37.6%	33.3%	22.7%	6.4%	53.0%	47.0%

On the positive-outcome end, as noted above, Energizer had the highest absolute pass rate at 48.5% with very low rates of not applicable (4.5%) and unknown (6.1%), giving a higher confidence that many controls were assessed and led to a segment-leading outcome. While the affirmative testing ratio placed Energizer the second-lowest pass ratio, it is worth noting that it had the most applicable & tested controls overall, leading to a segment-level skewing. The affirmative testing ratio result still puts Energizer, while lower, still within about 7%-points of the more performant cameras. Similarly, there was only about a 7%-point difference among the affirmative failure rates of these cameras.

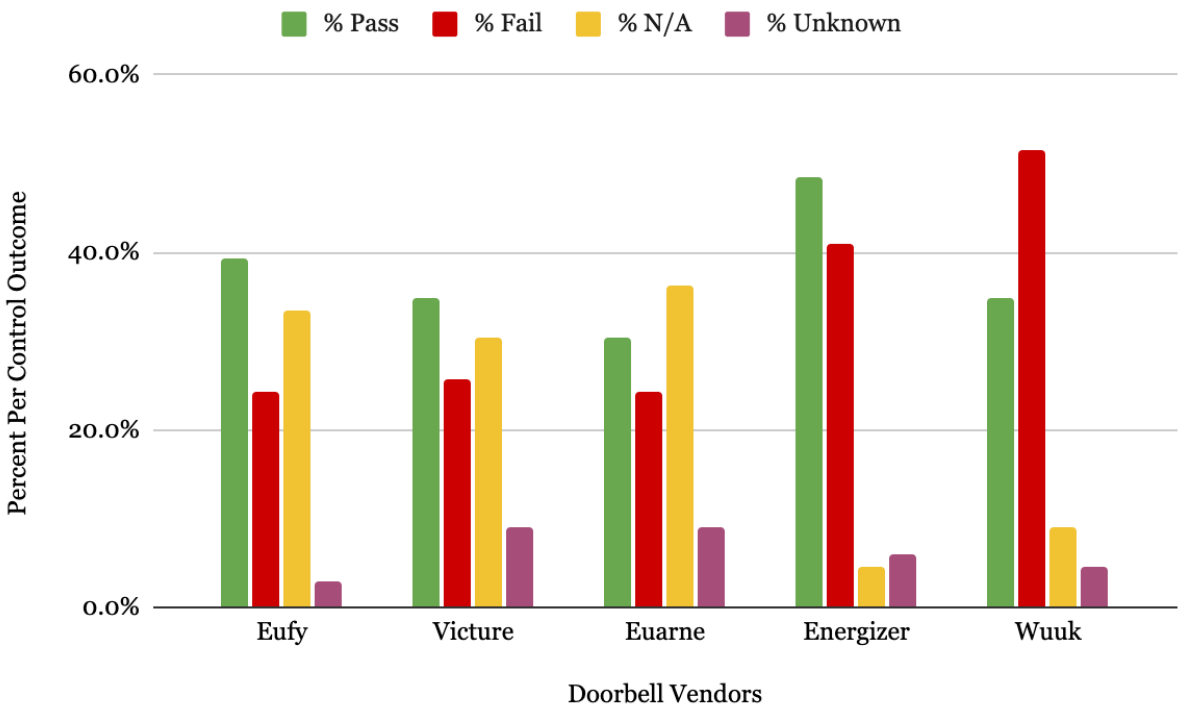

Figure 5. *Proposed framework - control outcomes for doorbells by vendor.*

Failure rates for the cameras with less applicability to control testing were tightly packed with less than 2%-points of variance for the absolute failure amount and about 6%-points of total variance in affirmative testing failure ratios, which can be better visualized in Figure 5. Similarly, these cameras also had similar ratios of controls that were not applicable or unknown.

Hidden Cameras

For the Hidden Camera segment (n=5) the survey sample device from Ecwey had the least favorable failure rate assessed for both absolute (60.6%) and affirmative testing outcomes (74.4%) across the segment. Similar results were seen from Pambrum and VicZone, which also had very high absolute (56.1% and 57.6%, respectively) and affirmative testing failure cases (71.2% and 70.4%, respectively), making these three cameras grouped tightly together. These

three cameras had very different levels of not-applicable and unknown result outcomes, making the conclusions drawn track so similarly across devices as shown in Table 8.

Table 8. *Proposed framework - hidden camera control outcome summary.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Camakt	28.8%	31.8%	9.1%	30.3%	47.5%	52.5%
Ecwey	21.2%	60.6%	9.1%	9.1%	25.9%	74.1%
Pambrum	22.7%	56.1%	21.2%	0.0%	28.8%	71.2%
Swept Supplies	24.2%	48.5%	22.7%	4.5%	33.3%	66.7%
VicZone	24.2%	57.6%	16.7%	1.5%	29.6%	70.4%
Average	24.2%	50.9%	15.8%	9.1%	32.3%	67.7%

On the favorable outcome side, all five cameras were grouped tightly in absolute pass numbers with a maximum variance of approximately 8%-points. This changes quite a bit when viewed through the lens of affirmative testing ratios where Camakt had a much higher pass rate at 47.5% compared to the next highest of Swept Supplies at 33.3%.

It's appropriate to note that Camakt had a very high set of unknown control outcomes (30.3%) and about 9% controls that were not applicable. Its absolute failure rate was the lowest (31.8%) by nearly 17%-points and affirmative failure ratio of 52.5% was over 14%-points lower than the next lowest number from Swept Supplies at 66.7%. While the controls to test were lower here by a decent margin compared to the other samples, all results highlight a better result for Camakt than any of the other vendors by a non-trivial difference.

If we review the result set for the hidden camera segment in Figure 6 it is further apparent how similar the failure outcomes were in absolute numbers for four-of-five sample devices, with further similarity in other control outcomes. Only Camakt has a strong degree of variance in the outcome percentages in any meaningful way.

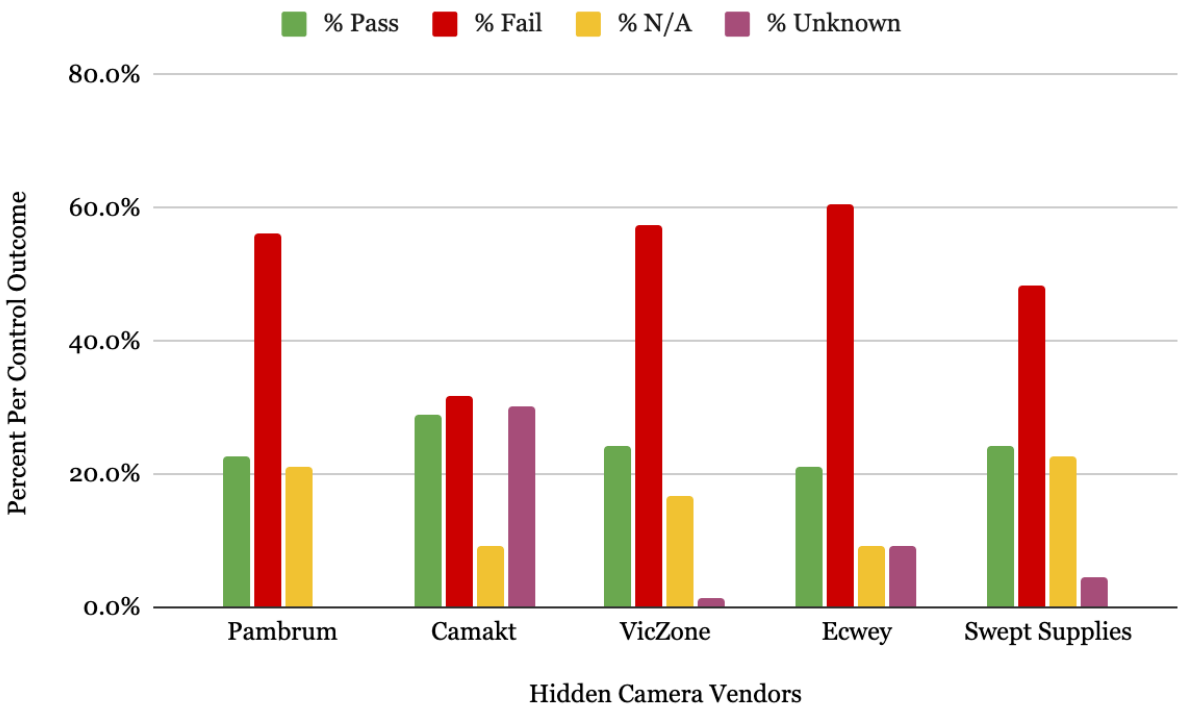

Figure 6. *Proposed framework - control outcomes for hidden cameras by vendor.*

Pet Feeders

Within assessed Pet Feeders (n=5) there was an extremely tight absolute failure rate with a variance of about 12%-points max and affirmative testing failures spread a maximum of under 10%-points. Similarly, favorable pass ratios were spread less than 8%-points and affirmative testing had a delta range within 9%-points. This range is rather compact for a segment's result set, especially when noting there was variance for not-applicable outcomes ranging from Sekoya's 6.1% to iSmartPet's 22.7%. Additional depth to these results is seen in Table 9.

Table 9. *Proposed framework - pet feeder control outcome summary.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Didog	28.8%	57.6%	13.6%	0.0%	33.3%	66.7%
HONGSA	28.8%	59.1%	10.6%	1.5%	32.8%	67.2%
IOIODOG	31.8%	47.0%	12.1%	9.1%	40.4%	59.6%
iSmartPet	24.2%	53.0%	22.7%	0.0%	31.4%	68.6%
Sekoya	31.8%	51.5%	6.1%	10.6%	38.2%	61.8%
Average	29.1%	53.6%	13.0%	4.2%	35.2%	64.8%

In positive absolute outcomes, Sekoya and IOIODOG shared the strongest result, both with 31.8%. IOIODOG had a slightly higher affirmative testing pass outcome with 40.4% against Sekoya's 38.2%. IOIODOG also had lower absolute and affirmative failure rates at 47.0% and 59.6%, respectively, compared to Sekoya's 51.5% and 61.8%. Through that lens, IOIODOG had the strongest pass rates with lower failure rates to the next closest sample. This is further supported due to small variances between the two devices for not-applicable and unknown result outcomes.

For less favorable results, HONGSA had a 59.1% absolute failure rate and 67.2% for affirmative testing. This is slightly worse than Didog's 57.6% and 66.7% results. Because these two vendors shared the same absolute pass rate of 28.8%, the results are even closer. Didog did have a slightly better (33.3% compared to 32.8%) affirmative pass rate. In general terms, these two devices are likely close to being equal for performing the least positively, but HONGSA may have slightly less performant results across the sample overall. The similarity of the larger sample in results can be seen in Figure 7 more readily.

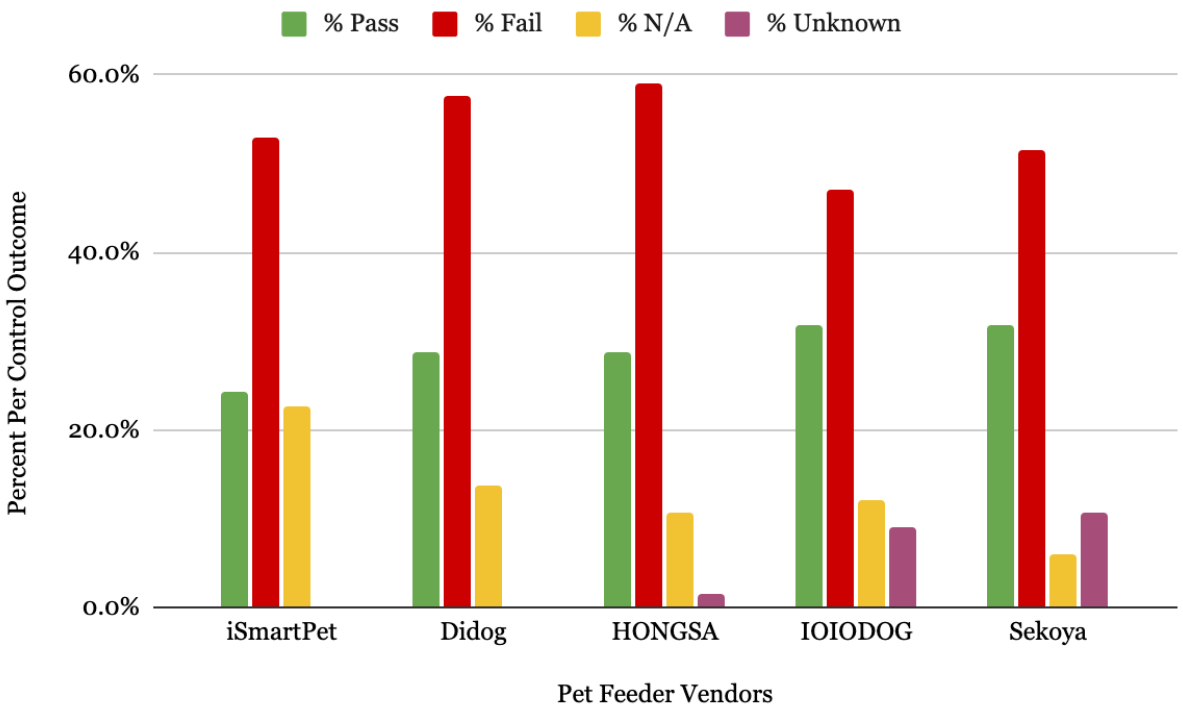

Figure 7. *Proposed framework - control outcomes for pet feeders by vendor.*

Security Cameras

The last market segment for analysis is that of Security Cameras (n=20). For the less favorable outcome, we can observe that Moonxiao has a 62.1% absolute failure rate and a 69.5% affirmative testing failure rate. That same sample device is also tied for the second lowest absolute pass rate of 27.3% and lowest affirmative pass rate of 30.5%. This makes a rather conclusive outcome that the Moonxiao sample of the 20 devices had the worst overall security compliance to the proposed framework's controls. A 0% unknown control result with a reasonable 10% not-applicable rate further this conclusion as can be seen in Table 10.

Table 10. *Proposed framework - security camera control outcome summary.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Akaso	40.9%	19.7%	30.3%	9.1%	67.5%	32.5%
Amcrest	30.3%	25.8%	3.0%	40.9%	54.1%	45.9%
Anbes	37.9%	22.7%	30.3%	9.1%	62.5%	37.5%
Anran	31.8%	57.6%	4.5%	6.1%	35.6%	64.4%
Aqara	39.4%	53.0%	6.1%	1.5%	42.6%	57.4%
Conico	34.8%	34.8%	28.8%	1.5%	50.0%	50.0%
DCT	33.3%	25.8%	34.8%	6.1%	56.4%	43.6%
Ecobee	45.5%	31.8%	16.7%	6.1%	58.8%	41.2%
Eversecu	25.8%	30.3%	34.8%	9.1%	45.9%	54.1%
Feit Electric	45.5%	37.9%	10.6%	6.1%	54.5%	45.5%
HeimVision	30.3%	60.6%	4.5%	4.5%	33.3%	66.7%
Jennov	27.3%	56.1%	15.2%	1.5%	32.7%	67.3%
LaView	31.8%	42.4%	16.7%	9.1%	42.9%	57.1%
Mascarry	33.3%	45.5%	16.7%	4.5%	42.3%	57.7%
Moonxiao	27.3%	62.1%	10.6%	0.0%	30.5%	69.5%
Reolink	37.9%	50.0%	12.1%	0.0%	43.1%	56.9%
StartVision	34.8%	19.7%	34.8%	10.6%	63.9%	36.1%
TP-Link	45.5%	47.0%	7.6%	0.0%	49.2%	50.8%
Vacos	31.8%	25.8%	37.9%	4.5%	55.3%	44.7%
WOHOME	33.3%	19.7%	36.4%	10.6%	62.9%	37.1%
Average	29.1%	53.6%	13.0%	4.2%	35.2%	64.8%

For positive security compliance the result is less obvious as there is a mixed result set of which devices performed the best against the proposed framework's criteria. In most cases, Akaso had the best result, but also tied for the 7th-highest not-applicable rate and (30.3%) and a non-trivial number of unknown results at 9.1%. Ecobee, Feit Electric, & TP-link tied for first for

the most favorable absolute pass rate with 45.5%. Of that group Ecobee had the lowest absolute failure rate with 31.8% and furthered its position with a 5th-highest affirmative testing pass rate, compared to 8th for Feit Electric & 11th for TP-Link. Failure rates with an affirmative testing for Ecobee was also lower with a 41.2% compared to Feit Electric's 45.5% and TP-Link's 50.8%.

Due to Akaso's high not-applicable rate for controls (30.3%) to Ecobee's much lower 16.7%, it is hard to discern a conclusive best result from this larger sample size easily. A lower unknown percentage for Ecobee – 6.1% compared to 9.1% for Akaso – may push Ecobee into a result that simply has more data behind its conclusion. Further depth to this data can be seen in Figure 8 to help compare this sample size more broadly.

Across the broader data set, absolute failure rates were showed the largest variance with a minimum of 19.7% for Akaso, StartVision, & WOHOME, while the maximum was Moonxiao's 62.1%, followed closely by HeimVision's 60.6% This 3x disparity end-to-end is stark when compared to other ratios that are primarily only a range of about double, end-to-end across the security camera sample. Seven devices had a not-applicable outcome rate of over 30% and an outlier of Amcrest showed 40.9% of unknown outcomes. That last number is almost 4x the next-largest number at 10.6% for StartVision & WOHOME.

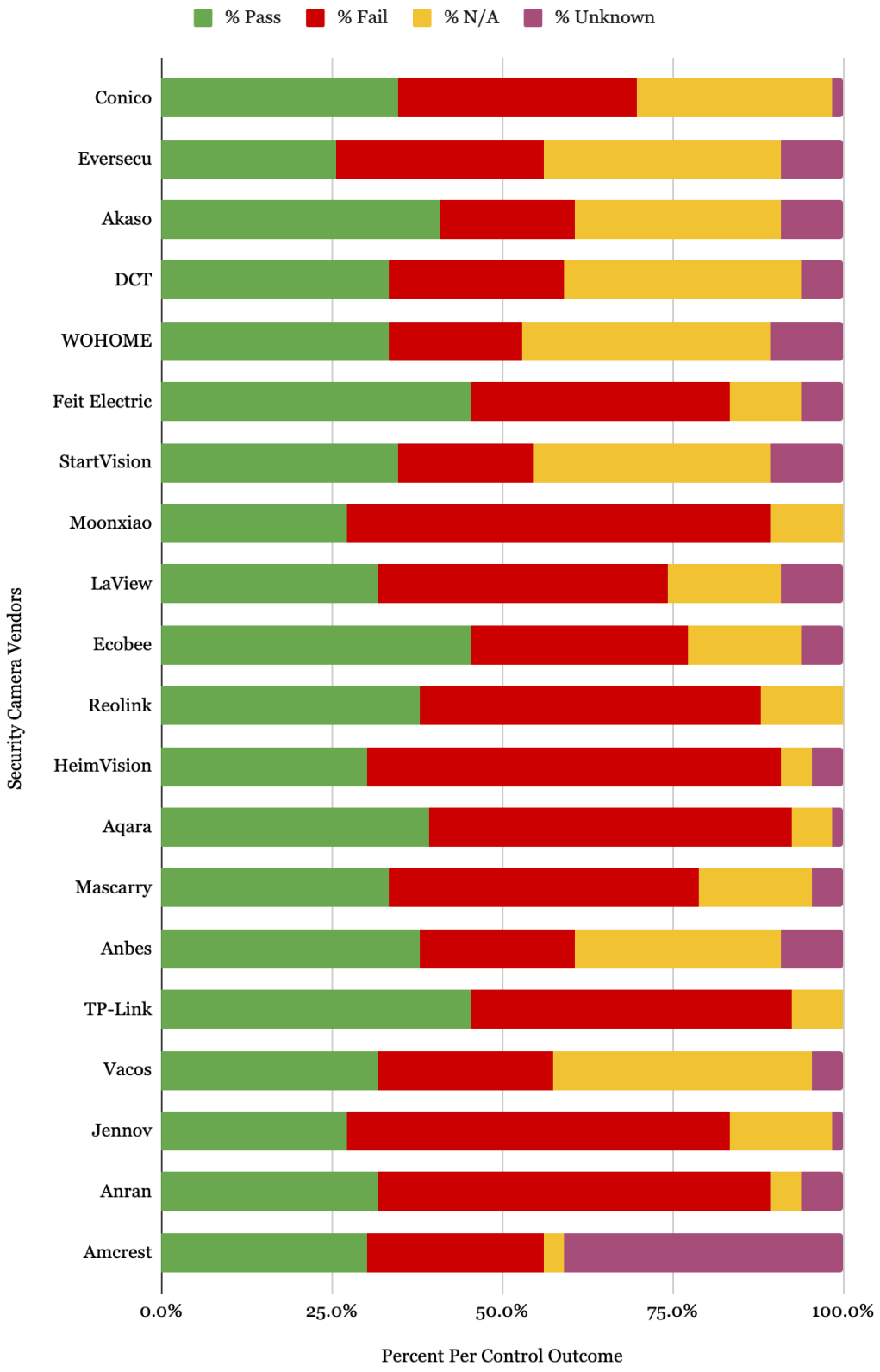

Figure 8. *Proposed framework - control outcomes for security cameras by vendor.*

Category-based Analysis

Within the proposed framework, a total of ten control categories are defined with the 66 controls spread across them. The proposed framework is then applied across the 40 devices within the survey, yielding 2,640 total results. In Table 11, the summary of those results can be seen. As is the case with segment-based testing, interpretation must consider applicability of categories to the sample devices, as well as testability yielding an affirmative result.

For instance, 11 devices within the survey are LiteOS-based, making Linux-specific test results not-applicable, which is denoted by the 27.8% result within this data set. Regarding data that is still unknown from testing, over 26% of firmware update tests were inconclusive due to the difficulty of assessing some firmware update mechanisms and/or there not being an update during the assessment window with which gathering such affirmative data was possible.

Table 11. *Proposed framework - category-based control outcome summary.*

Category	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Hardware Integrity	26.5%	73.5%	0.0%	0.0%	26.5%	73.5%
Local Access	41.5%	47.0%	11.5%	0.0%	46.9%	53.1%
Mobile Security	33.9%	46.8%	15.0%	4.3%	42.0%	58.0%
Wi-Fi Security	41.9%	42.5%	15.6%	0.0%	49.6%	50.4%
Service Security	43.2%	25.0%	31.1%	0.7%	63.3%	36.7%
Hardware Security	57.5%	24.4%	9.4%	8.8%	70.2%	29.8%
Firmware Updates	40.0%	20.6%	13.1%	26.3%	66.0%	34.0%
End-user Privacy	41.3%	50.8%	5.0%	2.9%	44.8%	55.2%
Binary Hardening	22.5%	45.0%	27.5%	5.0%	33.3%	66.7%
Linux Hardening	6.8%	57.3%	27.8%	8.3%	10.5%	89.5%
Average	35.5%	43.3%	15.6%	5.6%	45.3%	54.7%

Comparatively, “Hardware Integrity” had 0% not-applicable controls with “End-user Privacy” only having 5%. Seven-of-ten categories had 5%-or-less of controls that were fully unknown, highlighting that the remaining three categories were the bulk of unknown outcomes . In Figure 9 the distribution of control outcomes is much easier to consider. While “Linux Hardening” had less applicability, the results for what it did apply to show an extremely low 6.8% from absolute numbers. This can be further considered in the affirmative testing data above that shows a 10.5% pass rate, which removes LiteOS skew, but still shows a big issue.

“Binary Hardening” outcomes are also highly biased towards Linux-based OS results, but when viewed for affirmative testing results, a 33.3% outcome is yielded versus the 22.5% rate in absolute testing numbers. Again, the dramatic rise is due to removing the out-of-scope samples. Additionally, “Hardware Integrity” had a 26.5% affirmative testing pass rate, which was the second lowest outcome, sitting between “Linux Hardening” and “Binary Hardening” in the data.

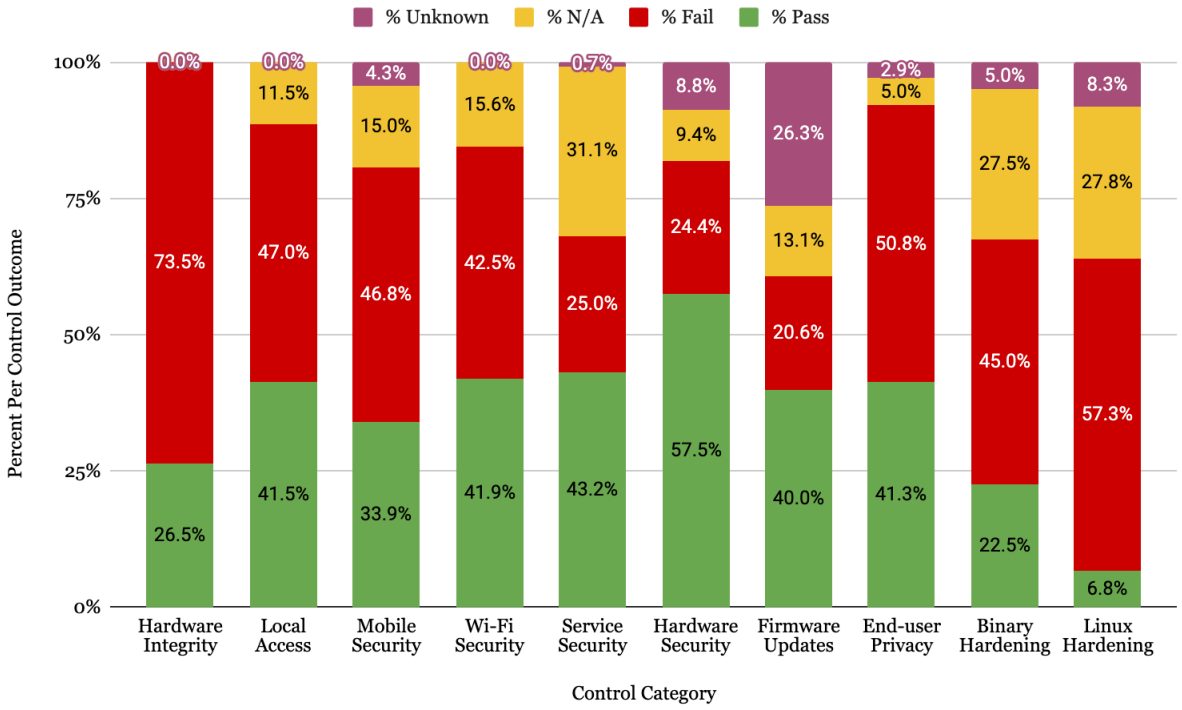

Figure 9. *Proposed framework - control outcomes by control category.*

Hardware security, on the other hand, had the strongest overall performance in absolute numbers at 57.5%, which is further validated with an affirmative testing pass rate of 70.2%. Two categories – "Firmware Updates" & "Service Security" both had affirmative testing pass rates above 60%, which were the only other categories that broke a 50% threshold for that type of analysis. Affirmative testing rates, however, show a more accurate picture of applicability for what was confirmed with rates such as "Firmware Updates" jumping from 40% to 66%.

Table 12. *Proposed framework - affirmative testing pass rate, per category, by segment.*

Category	Baby Monitors	Doorbells	Hidden Cameras	Pet Feeders	Security Cameras
Hardware Integrity	44.0%	32.0%	8.0%	4.0%	31.0%
Local Access	41.7%	54.2%	44.0%	44.0%	48.1%
Mobile Security	37.9%	53.1%	29.2%	35.7%	44.2%
Wi-Fi Security	66.7%	66.7%	20.0%	38.9%	53.7%
Service Security	73.5%	71.1%	50.0%	52.9%	64.6%
Hardware Security	68.4%	75.0%	70.6%	50.0%	74.6%
Firmware Updates	64.5%	70.8%	45.5%	56.5%	69.5%
End-user Privacy	50.0%	51.7%	32.1%	50.0%	43.8%
Binary Hardening	26.7%	33.3%	33.3%	30.0%	37.9%
Linux Hardening	13.0%	5.3%	10.5%	12.5%	9.5%
Average	48.6%	51.3%	34.3%	37.5%	47.7%

In Table 12 we can see a side-by-side of market segments' results for their respective affirmative pass rate. Some distinct take-aways can be gleaned, such as assessed Doorbells having a 5.3% pass rate overall, which is approximately 2x lower than any other segment. "Hardware Integrity" also stands out because while Baby Monitors show a 44% pass rate in this approach, Pet Feeders only have 4% and Hidden Cameras have 8%. The results of "Binary

Hardening" are also interesting because we see between 26.7% and 37.9% for affirmative pass rates, which is rather consistent for this topic.

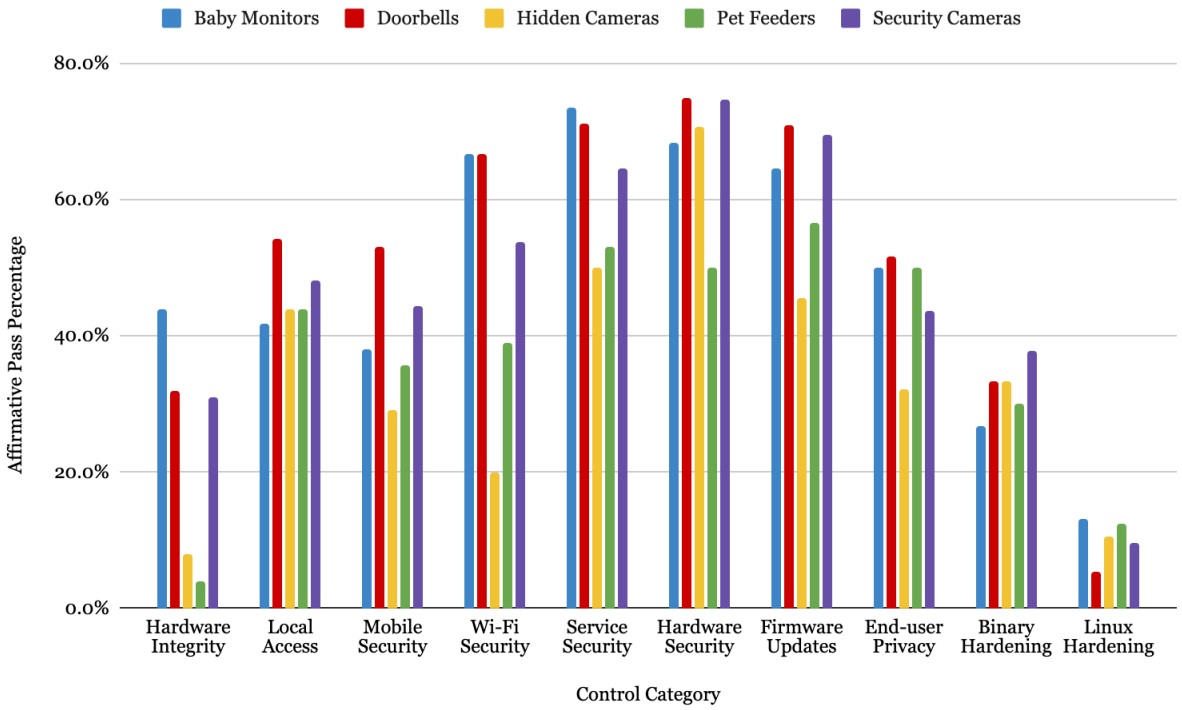

Figure 10. *Proposed framework - affirmative pass percentage, per category, by segment.*

When reviewing the data in Figure 10 we can more easily see where peaks & valleys in affirmative testing pass rates exist from the data. For instance, it is more apparent that "Wi-Fi Security" of Hidden Cameras are particularly weak relative to other segments. We can also discern that "Local Access" has a great degree of commonality between all segments, with Doorbells being slightly more favorable. Lastly, while "Service Security" is quite high in relative terms across segments, Hidden Cameras and Pet Feeders are both laggards across the markets.

Control-based Analysis

With the summary from Table 13, we can easily identify the proposed framework controls that were most prevalent for the various outcome types. For the *Pass* outcome set, all-

but-one device (Ecwey) did not allow for Wi-Fi to be configured via WPS (WF-01), which was the control that had the most adherence across the survey device sample. Conversely, HW-01 that provides physical tamper protection to the device failed across every device in the sample.

The controls that had the highest unknown result was the verification of a cryptographic hash for firmware updates (FW-07) at 52.5%. This result is due to the complexity of reverse engineering each specific firmware update mechanism, many of which are rather opaque when reviewing the runtime – if available to review at all.

For controls that were the least applicable across the survey sample, 87.5% of devices did not have MS-06 relevant to their testing. This is because the control is a secondary check that is dependent on MS-05 that necessitates a two-step verification capability in the first place, which only five vendors included with their associated mobile application and cloud service.

Table 13. *Proposed framework - most common controls for given outcome types.*

Most Passed	Most Failed	Most Unknown	Most Not-Applicable
WF-01 (97.5%)	HW-01 (100%)	FW-07 (52.5%)	MS-06 (87.5%)
MS-04 (95%)	WF-02 (100%)	FW-08 (50%)	SS-07 (80%)
SS-04 (95%)	SS-09 (97.5%)	FW-05 (47.5%)	SS-08 (80%)
EP-01 (95%)	EP-06 (95%)	LH-10 (32.5%)	SS-02 (62.5%)
SS-10 (92.5%)	LA-01 (92.5%)	FW-03 (30%)	WF-04 (62.5%)

Overall Camera Results

Across the entire survey sample (n=40) breaking down devices that are compliant to the proposed framework is quite difficult due to the wide range of not-applicable (2-25, with an average of 12) and unknown (3-27, with an average of 4) controls. If we slice the data a few ways, however, we may be able to infer some more reasonable conclusions.

For instance, Table 14 shows the top ten sample devices when sorted by affirmative testing pass rates. We can notice very high not-applicable control rates across many of these devices, which is mostly in the 30% range, with a notable exception of Ecobee. The average across the entire survey is a more modest 17.9% showing approximately a 2x increase.

Table 14. *Proposed framework - top ten survey devices by affirmative testing pass rate.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Akaso	40.9%	19.7%	30.3%	9.1%	67.5%	32.5%
StartVision	34.8%	19.7%	34.8%	10.6%	63.9%	36.1%
WOHOME	33.3%	19.7%	36.4%	10.6%	62.9%	37.1%
Anbes	37.9%	22.7%	30.3%	9.1%	62.5%	37.5%
Eufy	39.4%	24.2%	33.3%	3.0%	61.9%	38.1%
Ecobee	45.5%	31.8%	16.7%	6.1%	58.8%	41.2%
Victure	34.8%	25.8%	30.3%	9.1%	57.5%	42.5%
DCT	33.3%	25.8%	34.8%	6.1%	56.4%	43.6%
Euarne	30.3%	24.2%	36.4%	9.1%	55.6%	44.4%
Vacos	31.8%	25.8%	37.9%	4.5%	55.3%	44.7%

Reviewing Table 15 containing the top ten devices by their absolute pass rate across the proposed framework controls, we'll note that Ecobee comes in at second on the list, with a five-way tie for second in the list. Other devices in this list, such as the top-most Energizer, or others like Feit Electric, VTech, Kami Baby, and TP-Link are not found in our previous table structure. From the pass rate approaches between both tables, it is reasonable to conclude that Ecobee is the most favorable camera from the entire survey sample.

Failure rate analysis creates some overall doubt here due to the Ecobee coming in 16th most favorable for absolute failure testing and fifth through the view of affirmative testing for

failure outcomes. However, we must remember the Ecobee had a very low relative not-applicable control rate, which means it was assessed more closely across a broader control set.

Table 15. *Proposed framework - top ten survey devices by absolute testing pass rate.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Energizer	48.5%	40.9%	4.5%	6.1%	54.2%	45.8%
Ecobee	45.5%	31.8%	16.7%	6.1%	58.8%	41.2%
Feit Electric	45.5%	37.9%	10.6%	6.1%	54.5%	45.5%
VTech	45.5%	39.4%	13.6%	1.5%	53.6%	46.4%
Kami Baby	45.5%	39.4%	12.1%	3.0%	53.6%	46.4%
TP-Link	45.5%	47.0%	7.6%	0.0%	49.2%	50.8%
Motorola	43.9%	42.4%	9.1%	4.5%	50.9%	49.1%
Akaso	40.9%	19.7%	30.3%	9.1%	67.5%	32.5%
Eufy	39.4%	24.2%	33.3%	3.0%	61.9%	38.1%
Aqara	39.4%	53.0%	6.1%	1.5%	42.6%	57.4%

Alternatively, if we look at the absolute testing results for failure analysis in Table 16, we can discern that Moonxiao had the least favorable results with a 62.1% overall. A few other devices were close in the analysis, including Ecwey, HeimVision, and HONGSA, lagging 3%-points or less behind. Notably, Moonxiao has 0% unknown outcomes, giving this result even more applicability, especially compared to Ecwey's 9.1% unknown result, while the two shared very similar not-applicable outcome rates with Moonxiao at 10.6% and Ecwey at 9.1%.

Table 16. *Proposed framework - top ten survey devices by absolute testing failure rate.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Moonxiao	27.3%	62.1%	10.6%	0.0%	30.5%	69.5%
Ecwey	21.2%	60.6%	9.1%	9.1%	25.9%	74.1%
HeimVision	30.3%	60.6%	4.5%	4.5%	33.3%	66.7%

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
HONGSA	28.8%	59.1%	10.6%	1.5%	32.8%	67.2%
VicZone	24.2%	57.6%	16.7%	1.5%	29.6%	70.4%
Didog	28.8%	57.6%	13.6%	0.0%	33.3%	66.7%
Anran	31.8%	57.6%	4.5%	6.1%	35.6%	64.4%
Pambrum	22.7%	56.1%	21.2%	0.0%	28.8%	71.2%
Jennov	27.3%	56.1%	15.2%	1.5%	32.7%	67.3%
CellBee	33.3%	56.1%	10.6%	0.0%	37.3%	62.7%

When reviewing this same data through an affirmative testing view for failure rates as seen in Table 17, the ordering changes with Ecwey coming in at 74.1% and Moonxiao in the 4th least desirable position at 69.5% overall. This complicates a simple conclusion about which device may be least favorable against the proposed framework. It would be sufficient to state that Ecwey and Moonxiao both performed very poorly across the framework's controls.

Table 17. *Proposed framework - top ten survey devices by affirmative testing failure rate.*

Vendor	Pass	Fail	N/A	Unknown	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Ecwey	21.2%	60.6%	9.1%	9.1%	25.9%	74.1%
Pambrum	22.7%	56.1%	21.2%	0.0%	28.8%	71.2%
VicZone	24.2%	57.6%	16.7%	1.5%	29.6%	70.4%
Moonxiao	27.3%	62.1%	10.6%	0.0%	30.5%	69.5%
iSmartPet	24.2%	53.0%	22.7%	0.0%	31.4%	68.6%
Sense-U	24.2%	53.0%	21.2%	1.5%	31.4%	68.6%
Jennov	27.3%	56.1%	15.2%	1.5%	32.7%	67.3%
HONGSA	28.8%	59.1%	10.6%	1.5%	32.8%	67.2%
HeimVision	30.3%	60.6%	4.5%	4.5%	33.3%	66.7%
Didog	28.8%	57.6%	13.6%	0.0%	33.3%	66.7%

DCMS Framework Results

From the DCMS "Code of Practice for Consumer IoT Security" (U.K. Department for Digital, Culture, Media & Sport, 2018), a total of thirteen focuses are shared, nine of which were deemed in-scope for this study's intended data set. Unlike the proposed framework mapping exercise, the DCMS assessment does not leverage a *N/A* or *Unknown* outcome for a given control. Appendix F of this document provides a mapping for this framework that makes clear the relevant associations from this study's data set that provides the basis for a given result. Without analysis of this mapping, readers may draw inaccurate conclusions about the meaning.

In situations where data may not be known, a *Pass* result will be given to avoid erroneously marking controls as failed due to a lack of evidence from the data set. Because the control focus areas are not necessarily a straightforward one-to-one mapping, they would effectively need to be re-written to fully parse-out partial compliance. To this end, a *Fail* result may have more direct value to interpreting the data set since affirmative confirmation has been achieved. That's to say, if the result is a *Fail* outcome the control has been shown to have been failed, whereas a *Pass* result may have not had enough data to fully evaluate the control.

Lastly, due to only having nine assessed control areas for DCMS, the provided outcome percentages jump rather quickly. This lack of granularity makes applying the criteria from this guidance difficult for comparative analysis. In general, large gaps – or very low pass rates – are particularly relevant where two devices within 10%-points may not be that different in practice.

Overall Market-segment Analysis

Assessing DCMS findings through a market-segment view shows that Doorbells (n=5) have the strongest positive result with 60% passing outcomes. This is result is 5%-points higher than the next-best result of Security Cameras achieving 55%, but significantly higher than Pet

Feeders which had a 31.1% and represents the lowest segment result. Figure 11 represents a visualization for the distribution of outcomes across each of the market segments.

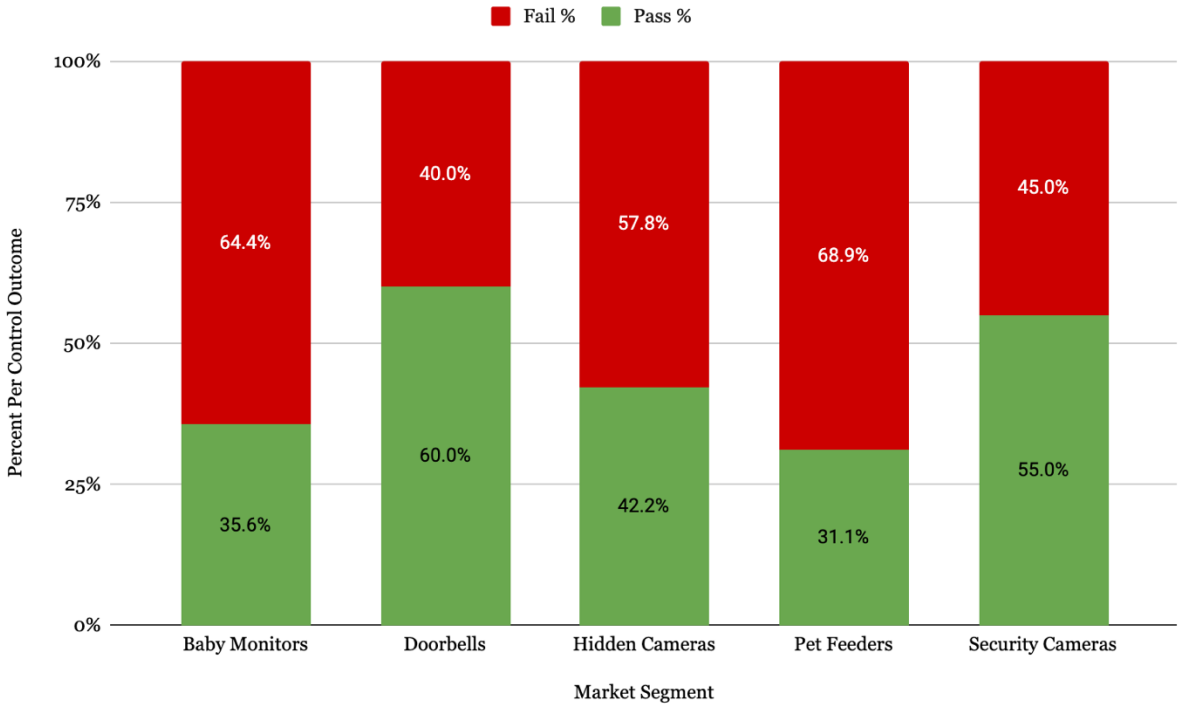

Figure 11. *DCMS - control outcomes by market segment.*

Individual Market-segment Analysis

Baby Monitors

For DCMS controls assessed, Baby Monitors (n=5) CellBee takes the lowest overall result with an 11.1% of passing assessed control criteria as shown by Table 18. The cameras across this segment represent quite a bit of distribution across the range of possible outcomes, with Motorola having a notably higher score than any other device by over 20%.

Table 18. *DCMS - baby monitor control outcome summary.*

Vendor	Pass	Fail
CellBee	11.1%	88.9%
Kami Baby	33.3%	66.7%
Motorola	66.7%	33.3%
Sense-U	44.4%	55.6%
VTech	22.2%	77.8%
Average	35.6%	64.4%

Doorbells

Within the Doorbells (n=5) market segment – which has the highest overall average of favorable results across segments – Eufy took the most favorable position with a 77.8% result. Energizer took the lowest spot with 44.4% as shown in Table 19, but in relative terms this is still much higher than all-but-one camera in the Baby Monitor segment, for instance.

Table 19. *DCMS - doorbell control outcome summary.*

Vendor	Pass	Fail
Energizer	44.4%	55.6%
Euarne	55.6%	44.4%
Eufy	77.8%	22.2%
Victure	55.6%	44.4%
Wuuk	66.7%	33.3%
Average	60.0%	40.0%

Hidden Cameras

Table 20 covering the Hidden Cameras (n=5) segment shows that Camakt had the highest pass rate (77.8%) of any device. It is worth noting for data bias considerations that the Camakt sample was lacking a great deal of affirmatively found data, which is likely skewing this result

for a lack of fully-conclusive findings. Still, relative to the overall population of devices that were between 22.2% (Pambrum) and 44.4% (Swept Supplies), this result is noticeably higher.

Table 20. *DCMS - hidden camera control outcome summary.*

Vendor	Pass	Fail
Camakt	77.8%	22.2%
Ecwey	33.3%	66.7%
Pambrum	22.2%	77.8%
Swept Supplies	44.4%	55.6%
VicZone	33.3%	66.7%
Average	42.2%	57.8%

Pet Feeders

When assessing Pet Feeders (n=5) the DCMS assessment results in Table 21 show that IOIODOG had the highest favorable outcome (55.6%) to the next closest cameras with both iSmartPet and Sekoya achieving a 33.3%. HONGSA, notably, had the least favorable result with an 11.1% overall for controls with a passing outcome, followed closely by Didog with 22.2%.

Table 21. *DCMS - pet feeder control outcome summary.*

Vendor	Pass	Fail
Didog	22.2%	77.8%
HONGSA	11.1%	88.9%
IOIODOG	55.6%	44.4%
iSmartPet	33.3%	66.7%
Sekoya	33.3%	66.7%
Average	31.1%	68.9%

Security Cameras

The final market segment of Security Cameras (n=20) in Table 22 highlights a broad distribution of results, which is helped by the larger device sample for this segment. The least favorable result is a tie between Moonxiao, Jennov, & Anran with a 22.2% pass outcome. Notably, Jennov & Anran were discovered during testing to be effectively the same camera, so this consistency makes sense. On the positive end of pass results, an impressive six devices – Akaso, Amcrest, DCT, Ecobee, StartVision, & WOHOME – all achieved a 77.8% of controls that had a passing outcome. 12-of-20 devices had a pass rate of higher than the average of 55%, highlighting that some of the lower performing devices pulled down the average quite a bit.

Table 22. *DCMS – security camera control outcome summary.*

Vendor	Pass	Fail
Akaso	77.8%	22.2%
Amcrest	77.8%	22.2%
Anbes	66.7%	33.3%
Anran	22.2%	77.8%
Aqara	33.3%	66.7%
Conico	66.7%	33.3%
DCT	77.8%	22.2%
Ecobee	77.8%	22.2%
Eversecu	66.7%	33.3%
Feit Electric	55.6%	44.4%
HeimVision	44.4%	55.6%
Jennov	22.2%	77.8%
LaView	55.6%	44.4%
Mascarry	44.4%	55.6%
Moonxiao	22.2%	77.8%
Reolink	33.3%	66.7%

Vendor	Pass	Fail
StartVision	77.8%	22.2%
TP-Link	44.4%	55.6%
Vacos	55.6%	44.4%
WOHOME	77.8%	22.2%
Average	55.0%	45.0%

Control-based Analysis

The results shown in Table 23 provides a summary of each control focus from the DCMS guidance with associated *Pass* and *Fail* rates representing the entire survey sample (n=40) that was assessed. The list below excludes four control areas that were deemed out of scope.

When analyzing the overall results, it is apparent that the highest failure rate comes from device vendors lacking a vulnerability disclosure policy that's readily available (ID 2). Only 10% of assessed vendor had such a policy discoverable, with Ecobee, Eufy, TP-Link, & Motorola achieving such an outcome. Conversely, 100% of vendors provided an instruction manual on how to setup and maintain their device, thereby achieving the base merit of that control (ID 11).

Of the remaining seven control focus areas, consumer deletion of data was the next strongest positive outcome with 67.5% adherence overall. In total, only four-of-nine controls reached a 50%-or-greater outcome for their focus areas' rate of achievement.

Table 23. *DCMS – summary by control outcome.*

ID	Control Focus	Pass	Fail
1	No default passwords	35.0%	65.0%
2	Implement a vulnerability disclosure policy	10.0%	90.0%
3	Keep software updated	50.0%	50.0%
4	Securely store credentials and security-sensitive data	40.0%	60.0%
5	Communicate securely	37.5%	62.5%

ID	Control Focus	Pass	Fail
6	Minimise exposed attack surfaces	47.5%	52.5%
7	Ensure software integrity	50.0%	50.0%
11	Make it easy for consumers to delete personal data	67.5%	32.5%
12	Make installation and maintenance of devices easy	100.0%	0.0%

When reviewing Figure 12 it is easier to observe that six-of-nine control focus areas are within 15%-points of one another for their pass rates.

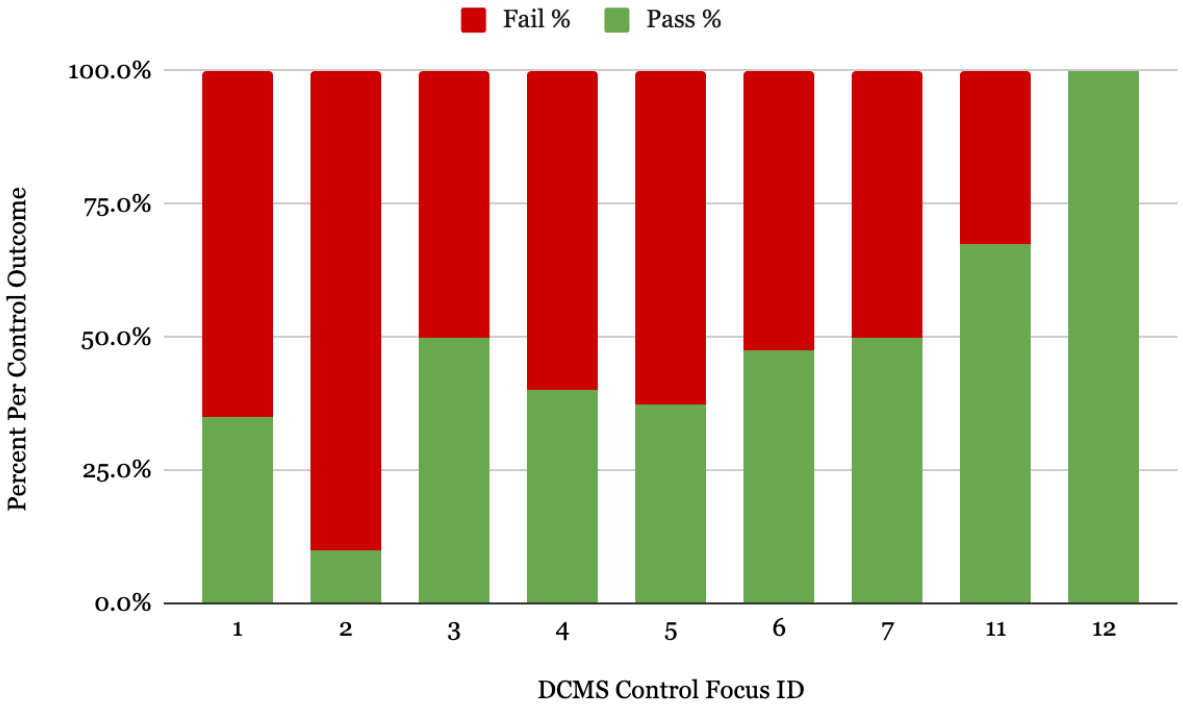

Figure 12. *DCMS – control outcomes by control identifier.*

Overall Camera Results

Across the survey sample devices (n=40) the DCMS assessment reflects that the strongest result is also the most favorable one with eight devices leading to a 77.8% pass rate. This, as noted prior, may have to do with the ability to test a given device fully and biasing towards a pass result when data was not present to disprove that as the outcome.

Notably, no device achieved a 100% adherence to the assessed guidance, nor did any device receiving a failing outcome on each of the nine control focus areas. We can observe in Figure 13 that with the limited number of controls to test for, there's a rather even distribution across the five possible percentage outcomes between our high-and-low results.

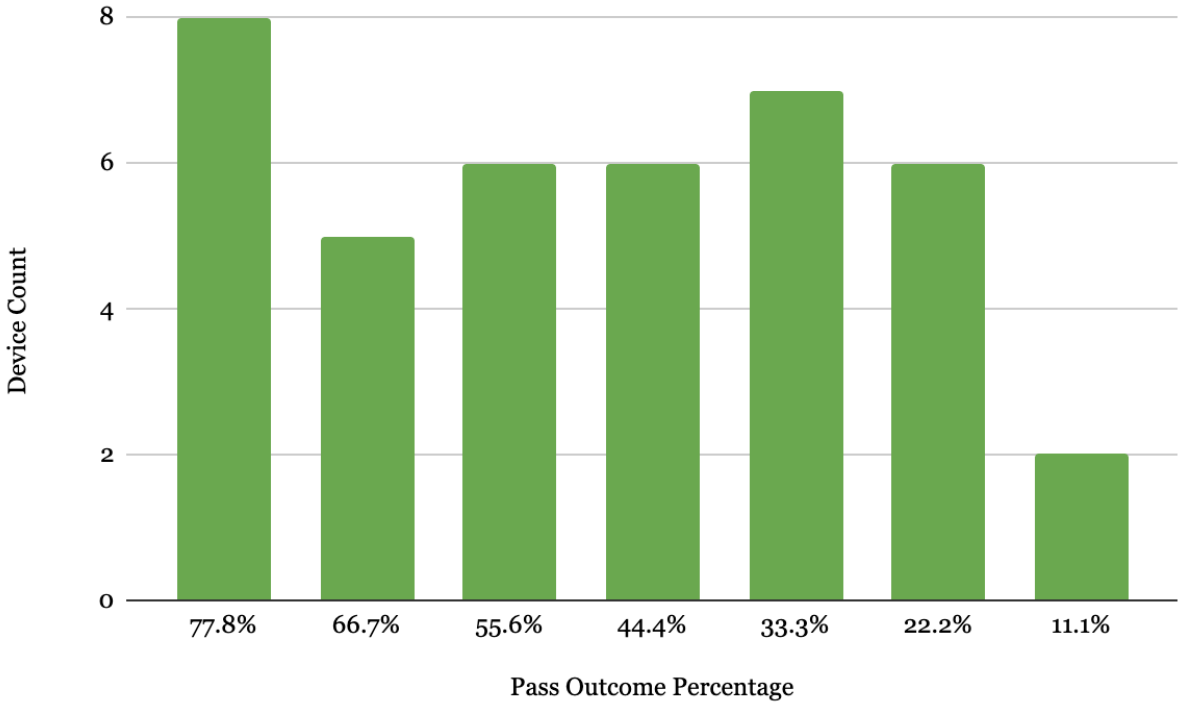

Figure 13. *DCMS – device count by passing outcome percentage.*

In Table 24, the 13 devices that achieved one of the top-two pass outcome percentages are shown. With 69.2% representation, Security Cameras (n=20) far outweigh other assessed market segments, which represent 50% of the total survey sample. Similarly, having two Doorbells (Eufy & Wuuk) representing 15% of the top 13 results outperforms the 12.5% of the sample that this segment contains. No assessed Pet Feeder (n=5) made this top 13 list devices.

Table 24. *DCMS - top 13 survey sample devices by outcome pass rate.*

Market Segment	Vendor	Pass	Fail
Doorbell	Eufy	77.8%	22.2%
Hidden Camera	Camakt	77.8%	22.2%
Security Camera	Akaso	77.8%	22.2%
Security Camera	Amcrest	77.8%	22.2%
Security Camera	DCT	77.8%	22.2%
Security Camera	Ecobee	77.8%	22.2%
Security Camera	StartVision	77.8%	22.2%
Security Camera	WOHOME	77.8%	22.2%
Baby Monitor	Motorola	66.7%	33.3%
Doorbell	Wuuk	66.7%	33.3%
Security Camera	Anbes	66.7%	33.3%
Security Camera	Conico	66.7%	33.3%
Security Camera	Eversecu	66.7%	33.3%

For sample devices that had the lowest percentage of DCMS control focus areas passed, a total of eight cameras makeup the two least favorable pass outcome rates at 11.1% and 22.2% as seen in Table 25. Compared to the favorable result set above where Security Camera inclusion was far-above its sample representation, only 37.5% of that market segment is shown, which is well below its 50% survey total. Baby Monitors & Hidden Cameras each had two devices appear on this list, representing 25% of this total view, which is above each of their segment's 12.5% total survey representation. Doorbells are the only market segment that does not make this less favorable summary. It is not until the 17th result in this view that a Doorbell (Energizer) is seen.

Table 25. *DCMS - bottom eight survey sample devices by outcome pass rate.*

Market Segment	Vendor	Pass	Fail
Baby Monitor	CellBee	11.1%	88.9%
Pet Feeder	HONGSA	11.1%	88.9%
Baby Monitor	VTech	22.2%	77.8%
Hidden Camera	Pambrum	22.2%	77.8%
Pet Feeder	Didog	22.2%	77.8%
Security Camera	Anran	22.2%	77.8%
Security Camera	Jennov	22.2%	77.8%
Security Camera	Moonxiao	22.2%	77.8%

ETSI Framework Results

The ETSI's "Cyber Security for Consumer Internet of Things: Baseline Requirements," EN 303 645 V2.1.1 (European Telecommunications Standards Institute, 2020) guidance provides a total of 62 controls across 13 categories. Of this list, 20 were deemed out-of-scope due to the research data set not being able to test for those conditions, or because the control guidance is simply being unrelated to the study's overall goals. Three categories are fully excluded because of this filtering and not included in any of the result sets below due to a lack of value.

Like the DCMS data mapping, the results of the ETSI control assessment will only provide a *Pass* or *Fail* outcome. Appendix C shares the detailed control mapping that shows what criteria from the study's assessment-tracking mechanism need to be met to achieve a passing outcome. The ETSI results also follow the DCMS assessment process in that they will provide for a passing result when data is inconclusive to map against. While the DCMS guidance had a few controls that needed a couple of criteria to provide a passing result, this guidance leads to a rather complex mapping structure yielding between one-and-six criteria to pass, per control.

Overall Market-segment Analysis

The ETSI assessment findings show in Figure 14 that Doorbells (n=5) were the best performing market segment with 70.5% controls that resulted in a passing outcome. On the less favorable end, Pet Feeders (n=5) had the lowest pass rate of all segments, with 37.5%. Hidden Cameras had a slightly better result with a 39.5% outcome pass rate for controls. Overall segment data for ETSI shows a rather wide overall distribution with the five assessed segments with passing outcome amounts that span 30, 40, 60, and 70-percentage results.

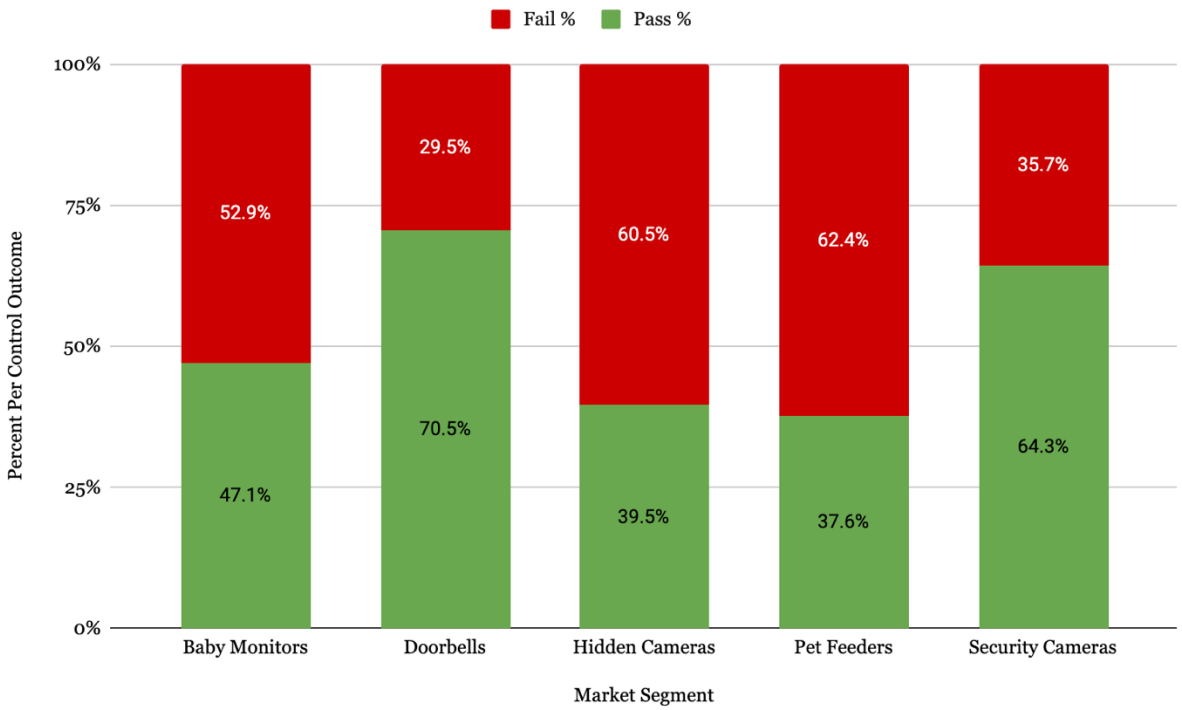

Figure 14. *ETSI - control outcomes by market segment.*

Individual Market-segment Analysis

Baby Monitors

Reviewing Table 26, we can see that of the assessed Baby Monitors (n=5) the sample device from Kami Baby had the strongest control pass rate with 64.2% overall. The least favorable device result of the segment came from CellBee with only 26.2% controls achieving a passing outcome. VTech was the only other device in the sample to receive a pass rate above the segment's average (47.1%) with a 59.5%, which is less than 5%-points than Kami Baby's result.

Table 26. *ETSI - baby monitor control outcome summary.*

Vendor	Pass	Fail
CellBee	26.2%	73.8%
Kami Baby	64.3%	35.7%
Motorola	42.9%	57.1%
Sense-U	42.9%	57.1%
VTech	59.5%	40.5%
Average	47.1%	52.9%

Doorbells

From the results of the Doorbell market segment (n=5), Table 27 shows a few extremely high control pass rates, including a tie at the top with 81% for both Euarne & Eufy. Wuuk also performed well, coming in less than 2.5% lower in overall pass rate, which is still quite strong at a 78.6%. The lowest pass rate of the segment was Energizer, which still achieved a 50% across the controls that were assessed. That result is just shy of the pass rate average across all segments (51.8%), so even the lowest segment result is still in a relatively healthy spot.

Table 27. *ETSI - doorbell control outcome summary.*

Vendor	Pass	Fail
Energizer	50.0%	50.0%
Euarne	81.0%	19.0%
Eufy	81.0%	19.0%
Victure	61.9%	38.1%
Wuuk	78.6%	21.4%
Average	70.5%	29.5%

Hidden Cameras

Within the results for Hidden Cameras (n=5) the pass-rate range is rather large, with the lowest result of 19% shared by both Pambrum & VicZone, up to the top spot with 88.1% for Camakt as shown in Table 28. As noted elsewhere, Camakt had a large amount of inconclusive data in testing so while that may account for some of the large disparity here, it is still over 2x as high as the next device, Ecwey with a 42.9%. The segment's 39.5% average was the second lowest and if it was not for Camakt's exceptional result, it would likely have exceeded Pet Feeders for overall failure rate.

Table 28. *ETSI – hidden camera control outcome summary.*

Vendor	Pass	Fail
Camakt	88.1%	11.9%
Ecwey	42.9%	57.1%
Pambrum	19.0%	81.0%
Swept Supplies	28.6%	71.4%
VicZone	19.0%	81.0%
Average	39.5%	60.5%

Pet Feeders

With the lowest overall segment average of the survey at 37.6%, Pet Feeders (n=5) had several low pass rates for devices. The lowest result was a 19% for iSmartPet with HONGSA at a slightly better 21.4%. More favorably, IOIODOG received a 78.6%, helping to bolster the segment's overall average as seen in Table 29, which is still extremely low in relative terms.

Table 29. *ETSI - pet feeder control outcome summary.*

Vendor	Pass	Fail
Didog	28.6%	71.4%
HONGSA	21.4%	78.6%
IOIODOG	78.6%	21.4%
iSmartPet	19.0%	81.0%
Sekoya	40.5%	59.5%
Average	37.6%	62.4%

Security Cameras

Security Cameras (n=20) unsurprisingly had quite a range of results as shown in Table 30 with its large sample size. WOHOME & StartVision both had assessment results showing a pass rate of a staggering 92.9% with Eversecu close behind at 90.5%. On the low end of passing control outcome rates, Jennov had a 16.7% result. Interestingly, only four devices achieved a result higher than the overall segment average of 77.1%, including the already-noted cameras, as well as DCT and Vacos. As noted, controls that are unable to be tested or not relevant do not penalize a camera's results, which may lead to unexpected data outcomes.

Table 30. *ETSI - security camera control outcome summary.*

Vendor	Pass	Fail
Akaso	69.0%	31.0%
Amcrest	71.4%	28.6%
Anbes	64.3%	35.7%
Anran	33.3%	66.7%
Aqara	35.7%	64.3%
Conico	59.5%	40.5%
DCT	83.3%	16.7%
Ecobee	66.7%	33.3%
Eversecu	90.5%	9.5%
Feit Electric	76.2%	23.8%
HeimVision	52.4%	47.6%
Jennov	16.7%	83.3%
LaView	73.8%	26.2%
Mascarry	69.0%	31.0%
Moonxiao	38.1%	61.9%
Reolink	61.9%	38.1%
StartVision	92.9%	7.1%
TP-Link	61.9%	38.1%
Vacos	76.2%	23.8%
WOHOME	92.9%	7.1%
Average	77.1%	22.9%

Category-based Analysis

In Table 31, a summary of ETSI categories – ten in total – represent a total of 1,680 total assessments across the survey's device sample (n=40) due to the 42 in-scope controls. A notable result is that category 5.12, which only has one control related to the availability of device configuration guidance (i.e., a user manual). Beyond that outlier, the most favorable outcome

was a tie between 5.15 – regarding software integrity – and user data deletion in category 5.11. Software updates came in closely behind with 66.3%. The category that represented the least desirable pass rate was 5.4, which had a 16.3% result and relates to the secure storage of data.

Table 31. *ETSI - category-based control outcome summary.*

ID	Category	Pass	Fail
5.1	No universal default passwords	44.0%	56.0%
5.2	Implement a means to manage reports of vulnerabilities	20.0%	80.0%
5.3	Keep software updated	66.3%	33.8%
5.4	Securely store sensitive security parameters	16.3%	83.8%
5.5	Communicate securely	53.2%	46.8%
5.6	Minimize exposed attack surfaces	64.6%	35.4%
5.7	Ensure software integrity	67.5%	32.5%
5.8	Ensure that personal data is secure	45.0%	55.0%
5.11	Make it easy for users to delete user data	67.5%	32.5%
5.12	Make installation and maintenance of devices easy	100.0%	0.0%
	Average	54.4%	45.6%

When reviewing the ETSI sample results visually with Figure 15, we can more-easily note that three-of-ten categories had results within the 60%-point range. Category 5.2, which ties back vulnerability management by vendors, had another very low result with only 20% of sample devices meeting that requirement. Both 5.1 & 5.8 had a pass rate in the mid-40% range, which are the other two categories that fell below the overall average across categories of 54.5%.

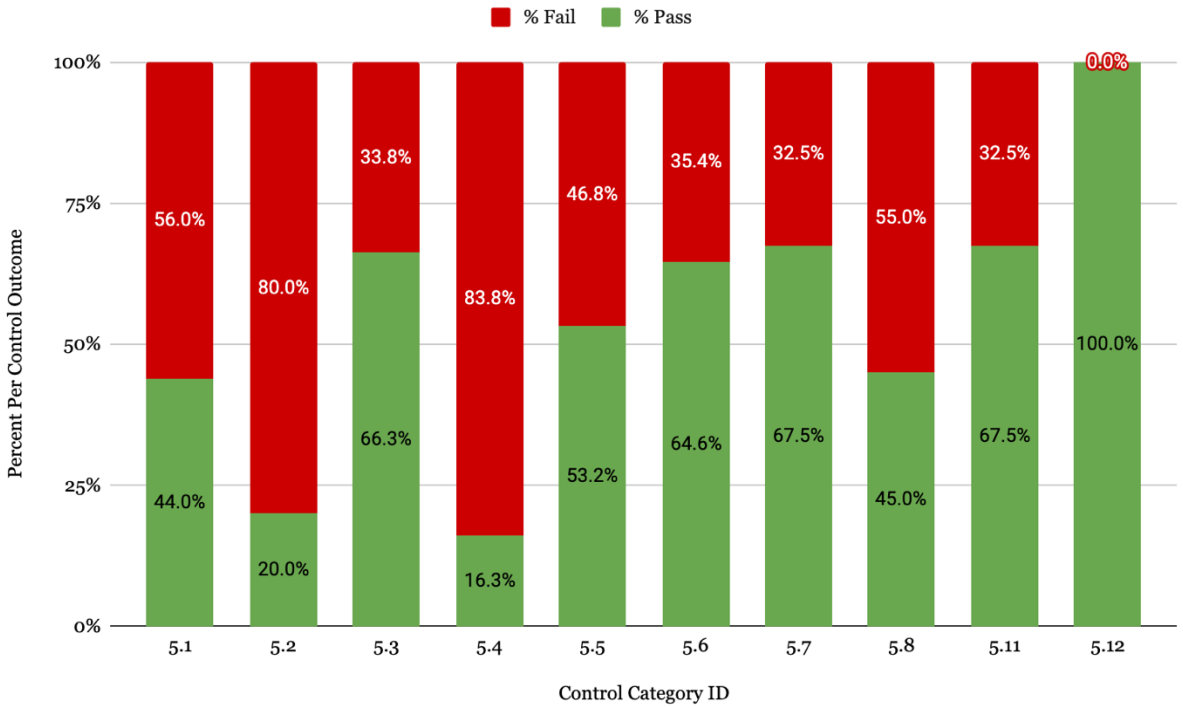

Figure 15. *ETSI - control outcomes by control category.*

In Figure 16, sample market segments are shown highlighting their pass rate for the denoted category IDs on the horizontal axis. One notable outcome is that Hidden Cameras have a 100% achievement for control 5.11, which is not seen for any control except 5.12 otherwise. Doorbells also have several higher peaks of adherence across six-of-ten categories. We can also note that Pet Feeders and Baby Monitors have some notably weak results in many categories.

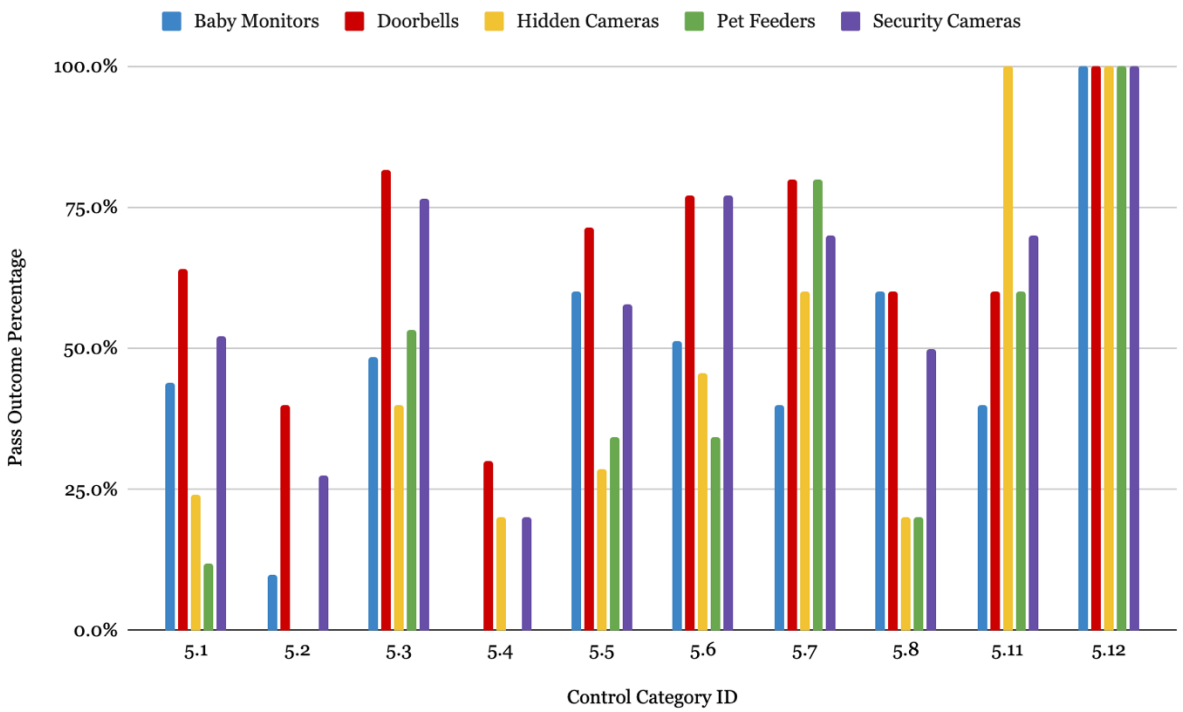

Figure 16. *ETSI - pass percentage, per category, by segment.*

Control-based Analysis

For 42 assessed controls within the ETSI per sample device, Table 32 highlights both the best, and worst, ten controls when assessed by their sample-wide pass rate. In addition to category 5.12 mentioned prior, three other controls – 5.3-16, 5.6-3, & 5.6-8 – each had a 100% pass rate across the device survey sample (n=40). The first identifier relates to the device having a model designation, which all devices acquired had some sort of designation (albeit less unique in some cases). The second and third identifier relate to a few different hardware security aspects, including limiting external device attack surface and CPU memory control.

For the lower-end of pass rates, only one device had obvious usage of 5.4-1, which relates to secure parameter store (e.g., TPM). Another very low control pass rate was 5.2-1 which was mentioned (in part) related to an overall low category success rate prior. This control

specifically relates to vulnerability report handling by the vendors of the sample devices. The next eight lowest pass rates were all within 8% of each other, covering five-of-ten categories.

Table 32. *ETSI - top-and-bottom ten survey sample devices by outcome pass rate.*

Most Passed			**Least Passed**	
5.3-16 (100%)	5.5-3 (85%)		5.4-1 (2.5%)	5.6-7 (32.5%)
5.6-3 (100%)	5.3-9 (82.5%)		5.2-1 (10%)	5.1-2 (35%)
5.6-8 (100%)	5.5-4 (77.5%)		5.6-4 (27.5%)	5.5-1 (37.5%)
5.12-2 (100%)	5.6-1 (77.5%)		5.2-3 (30%)	5.5-2 (37.5%)
5.3-3 (85%)	5.6-5 (77.5%)		5.4-3 (30%)	5.6-9 (37.5%)

Overall Camera Results

Reviewing Figure 17 readily highlights where each sample device came out in terms of total control assessment outcomes by their pass-and-fail percentages. WOHOME & StartVision took the top spot with a 92.9% pass rate, followed closely by Eversecu with a 90.5% result. Only seven sample devices found themselves within the 80%-point or greater range.

When analyzing the results of the lowest pass rates across vendors, Jennov had the least favorable score with a 16.7%, followed by Pambrum, iSmartPet, & VicZone each with 19%. Of the total survey sample (n=40), 17 devices fell below the average pass rate percentage of 56.5%.

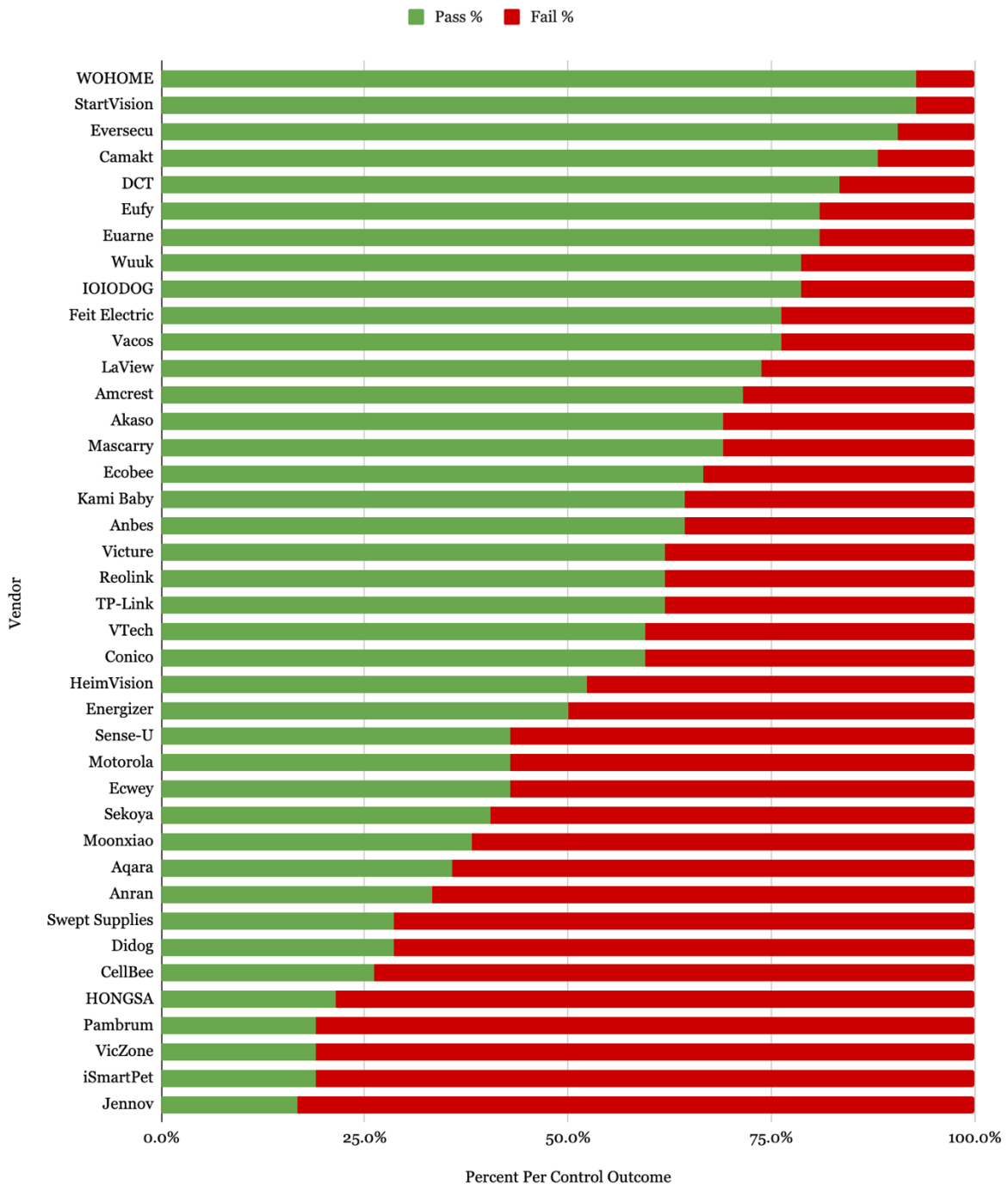

Figure 17. *ETSI - control outcomes by vendor.*

Camera Scoring Rollup

In analysis of this research study's data against the three chosen frameworks – proposed framework, DCMS, & ETSI – it is worth considering how the outcomes from each assessment may correlate or differ when viewed through a more unified lens. Because of ranking variance and overlap in an individual framework, we can take an approach to add individual framework percentage outcomes together across the three frameworks for a given sample device to compute an aggregate score. That score then can be compared to other devices since the total possible across the frameworks would be 300%. This allows a basic ranking to be asserted across results.

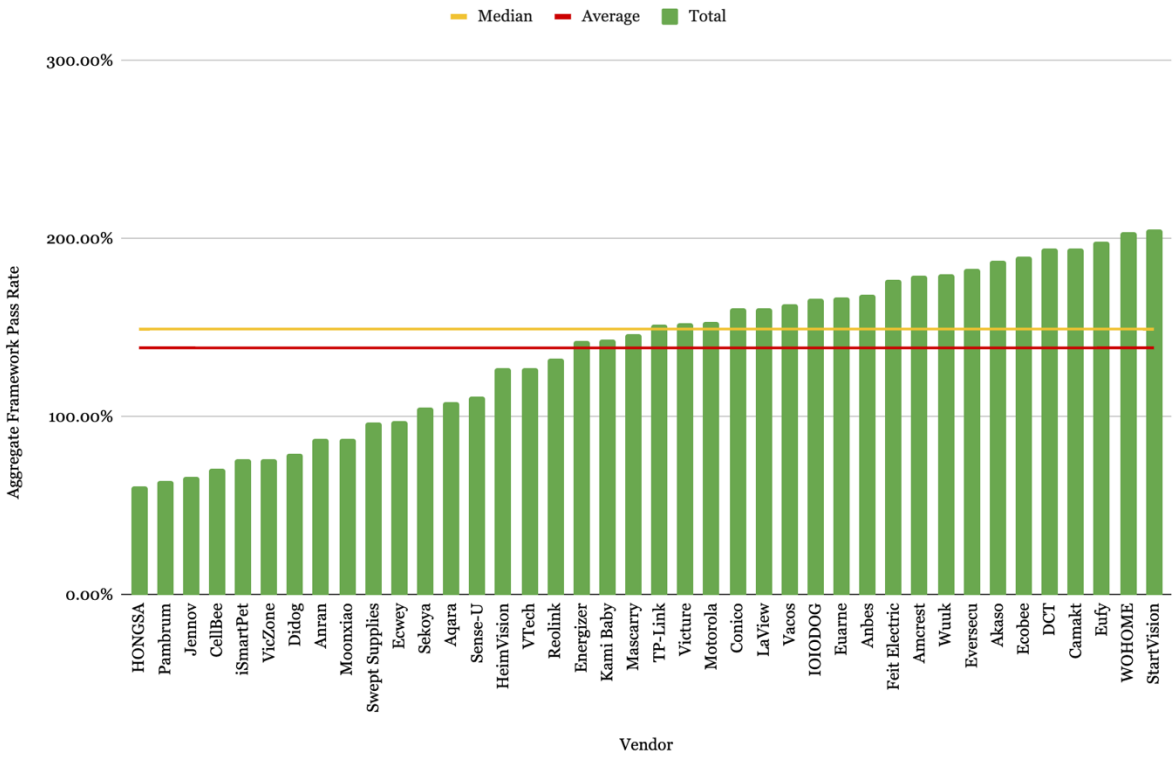

Figure 18. *Aggregate framework pass rate by vendor.*

Reviewing Figure 18 we can easily determine that StartVision (205.5%), WOHOME (204%), Eufy (198.1%), Camakt (194.7%), & DCT (194.4%) had the five highest total

composite pass-rate percentages across the three frameworks. On the lower-end, we can see that HONGSA (61.3%), Pambrum (64%), Jennov (66.2%), and CellBee (70.6%) took the four lowest spots, with iSmartPet, VicZone, & Didog tying for the fifth spot with 76.6%. In total, 23-of-40 cameras exceeded the average (138.7%) and 20-of-40 exceeded the median (149.3%). That final statistic is of interest since represents exactly half of our total survey sample and fell equally on opposite sides of the median line from this composite scoring approach.

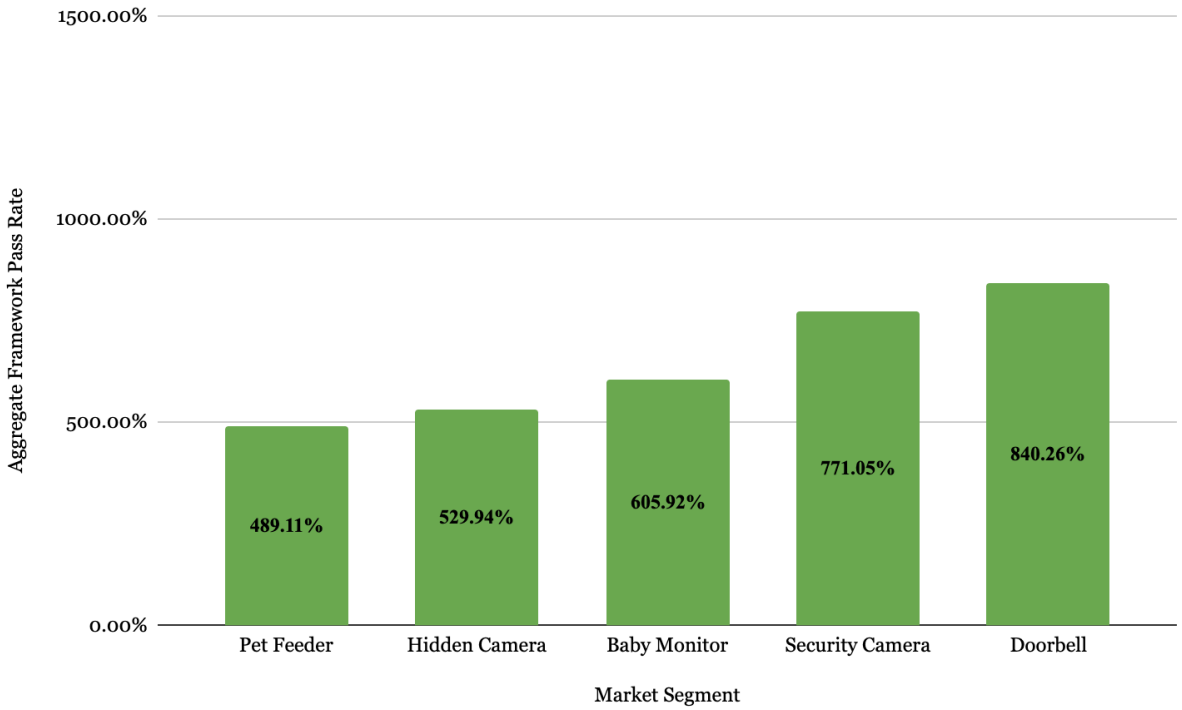

Figure 19. *Aggregate framework pass rate by market segment.*

In another approach, we can aggregate a market segment's results across cameras to provide a composite view of pass rates. Segments with five cameras and a maximum pass rate between frameworks of 300% means that 1,500% is possible in aggregate. The exception here is with the Security Cameras segment, due to its 20-device sample size. To normalize our data for analysis, that market segment is divided by four to end up with a 1,500% upper bounds, too.

We can see that at a market segment-level in Figure 19, the Doorbell sample comes out ahead with 840.26% of a possible 1,500%. This was followed rather closely by Security Cameras at 771.05%. On the less favorable side, Pet Feeders came in at 489.11% with Hidden Cameras nearby at 529.94%. Notably, dividing this total range into equal parts – 0-375%, 375-750%, 750%-1,125%, and 1,125%-1,500% – all results fall within the middle two ranges. From that we can better understand that while there exist non-trivial relative disparities in outcomes, there is a rather tight grouping across segments in the sense of absolute aggregation ranges.

When we review previous segment data, we can see that Doorbells & Pet Feeders share some parity with equal – albeit opposite – absolute positionings across frameworks. Doorbells took the most favorable spot for ETSI & DCMS with a 2nd-best outcome for the proposed framework. Pet Feeders had the same structural outcomes on the less-favorable end of results. This comparative analysis helps provide further assurances that these segments, for their respective outcomes, are rather stable when we review our data from different perspectives.

While the total difference between Doorbells and Pet Feeders is 351.15% across 1,500% possible, a more valuable way to review that disparity is that Doorbells had a 72%-higher total composite score when compared to Pet Feeders. In relative terms, this is quite a wide gap. Because of the tight coupling of composite pass rates between market segments, we can discern that segments themselves are neither completely devoid of security overall, nor are they doing a particularly excellent job of it on scale, when assessed with these frameworks and data sets.

Data Analysis Questions

Beyond the data comparisons provided at the framework-to-framework level, the data and framework analysis results can be used to answer other questions of possible interest. For instance, Figure 20 helps to highlight how the composite framework analysis results map against

the price ranges for devices within the survey sample. As a reminder, all assessed cameras were approximately $50 to $150, providing effective boundaries to the overall range.

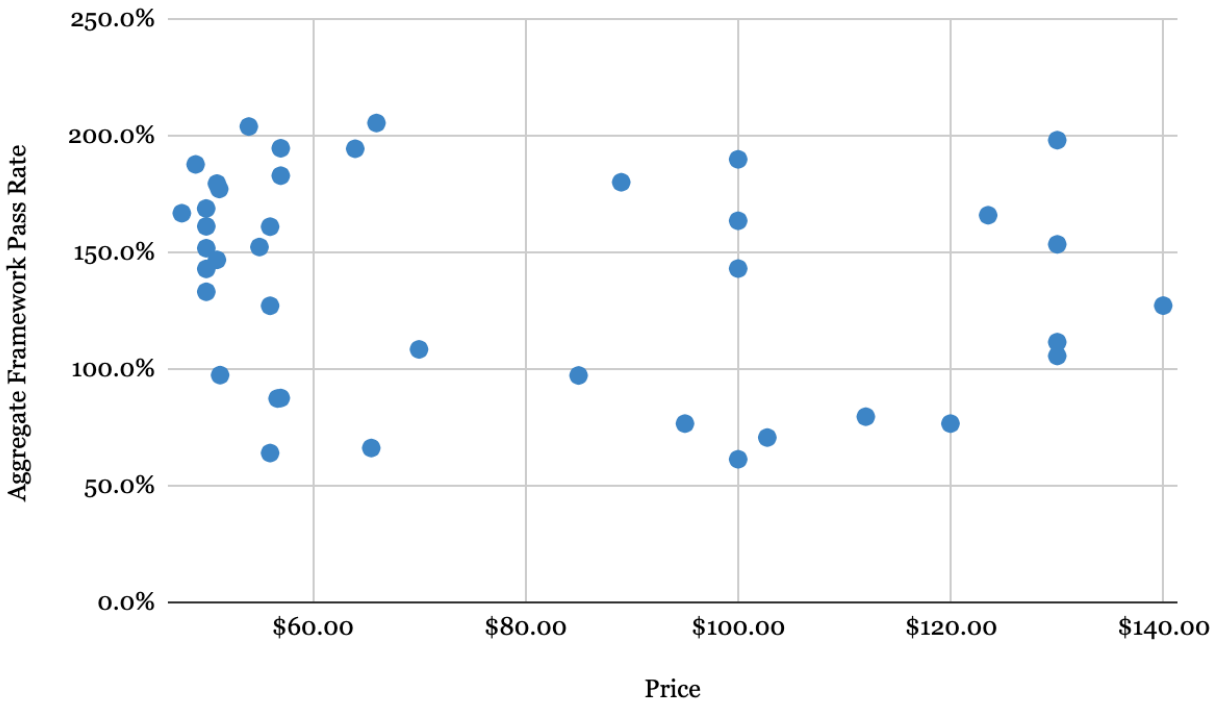

Figure 20. *Aggregate framework pass rate by device price.*

In this plot we can observe that 20 of the survey's cameras – half of the total sample – were under $60 in price. As noted, 138.7% is the average of the composite framework totals from assessed devices, which from this visualization we can observe that 15-of-20 cameras from that price point threshold is above our average. This is notable because we can discern that 75% of the $60-or-less price point devices are above average in terms of composite security analysis scoring. 15-of-40 cameras are under the average, allowing us to note that the price of a camera does not appear to have any clear correlation to the security of a device as it relates to the IoT security frameworks and scoring methodology used within this overall research study.

Another question we can explore is if vendors which have a published security policy are making devices that are stronger in assessed security than devices that do not have that approach. We can map our four vendors in Figure 21 that have such a published policy – Ecobee, Eufy, TP-Link, & Motorola – against the average (138.7%) from the overall survey sample. It is easy to see in this approach that each of the cameras exceed the overall average for all devices. Many devices are of course also above this average but having 100% of this portion of the sample at least provides a correlation between that vendor security policy and better outcomes.

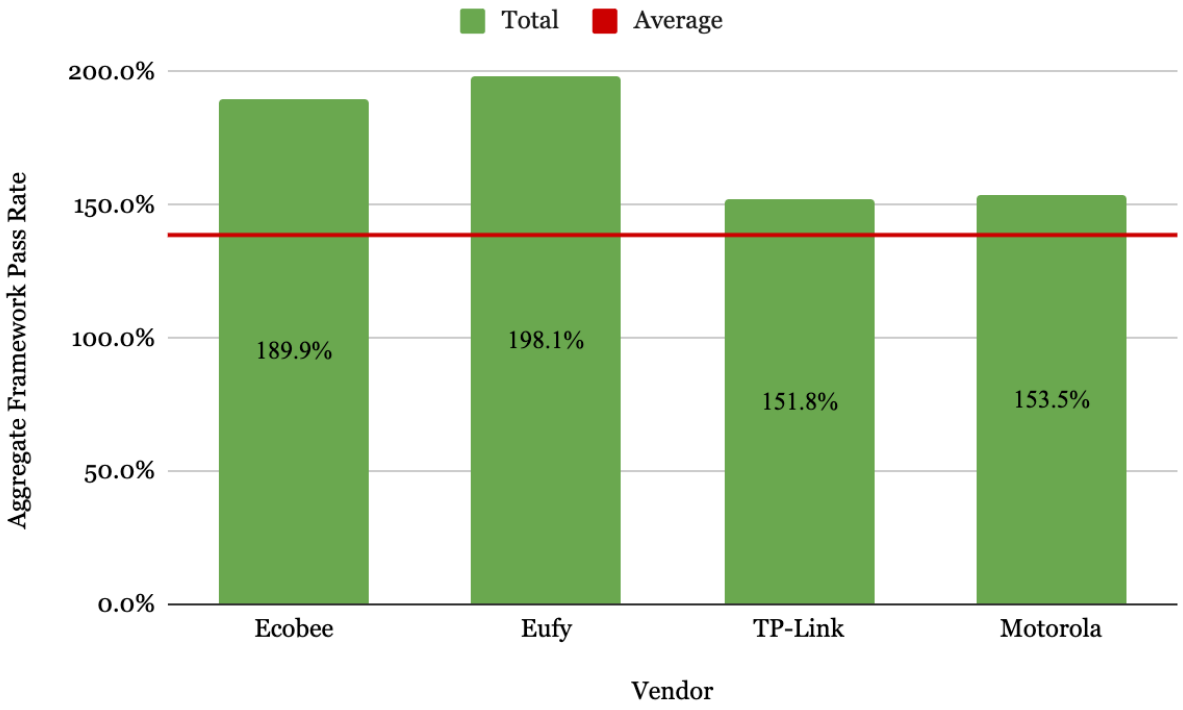

Figure 21. *Aggregate framework pass rate for vendors with a security policy.*

A final question we can consider is whether vendors that make claims about their camera's security – either on packaging or in the user manual – have higher-than-average composite security totals. In Figure 22 we're able to plot the 11 cameras from the sample that had such vendor security claims with the overall sample's average (138.7%) placed in. A total of eight cameras (72.7%) of that cohort is above the overall average. This result shows a reasonable

correlation that vendors providing these claims are exceeding the overall average. Such vendor claims help to provide consumer awareness of IoT security expectations but requires this empirical analysis of those claims to establish that trust by those consumers is well informed.

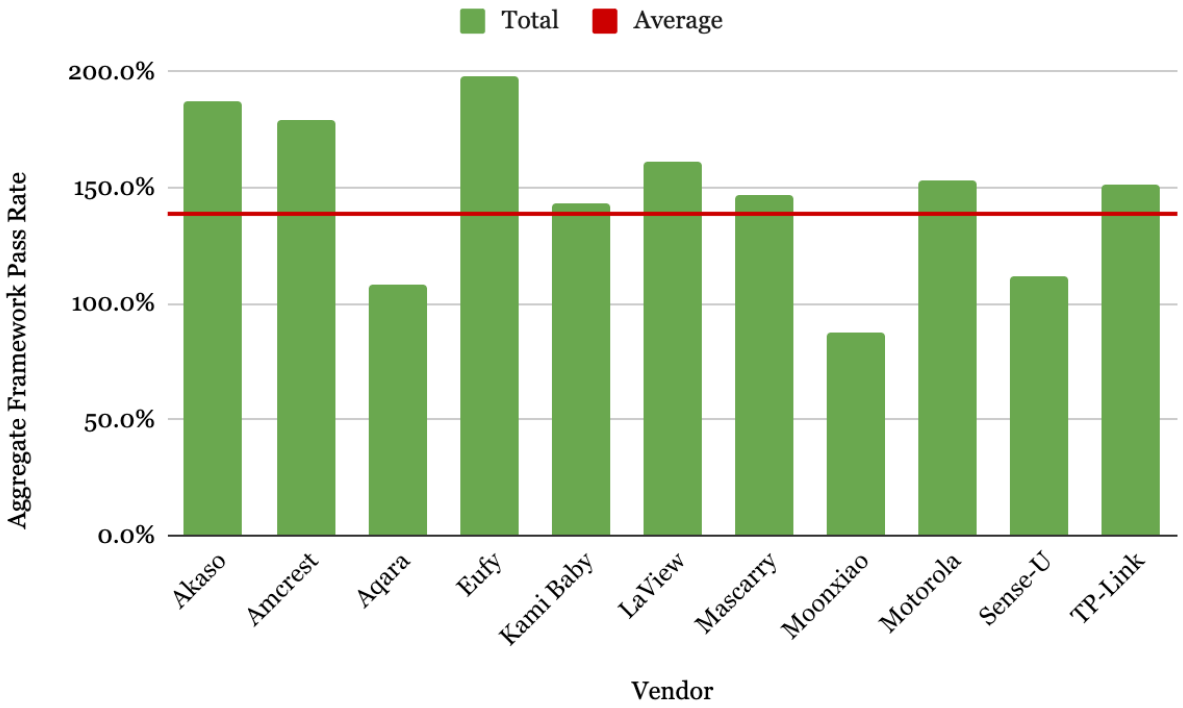

Figure 22. *Aggregate framework pass rate by vendors making security claims.*

Additional questions from the raw data set could also be derived and do not necessarily need to involve the IoT security framework mapping analysis. For instance, determining correlations that may exist between certain chipsets, OS choices, or network service existence.

CHAPTER 5

CONCLUSION

In this final chapter, contributions to the literature are enumerated and study limitations are explained. Future research ideas that would complement this research agenda's outputs, as well as a summary, will also be shared.

Contributions

1. **Device Assessment Methodology:** The data gathering exercise for this dissertation across the IoT camera device sample (n=40) required a consistent approach on a per-device basis to ensure that all applicable elements were gathered as efficiently as possible. While a given device's unique properties may change some of the techniques utilized to achieve that data gathering, the overall process, tools, and approaches were very similar in nature. The contribution to the literature of this process will help to enable other researchers to simplify their own efforts to gather similar data for additional device samples, which may reduce the burden to contribute their own data back as well.
2. **Device Results:** The assessed device samples provide the research community with a wide range of data about various security, privacy, configuration, mobile, and hardware properties for devices assessed. This is meaningful because of the size of the sample, the relative uniformity of the sample as defined by the research's constraints, the number of data elements shared about each device (up to 139 in total), and the methodology that was followed to ensure quality and consistency of the data. As noted in the literature review, prior research often had limited raw insights about devices and often instead focused on

exploitation rather than meta data that could be used to draw inferences. This data set can now provide researchers with real-world data over a non-trivial sample size with which they may draw their own conclusions about the devices assessed, the market segments represented, and the approaches to security that were (or were not) followed.

3. **Newly Proposed IoT Security Framework:** Appendix A of this dissertation provides for a custom IoT security framework that aims to address some of the gaps that were noted during the usage of existing industry-provided offerings. This 66-control framework attempts to provide a broad, impactful, and simply written set of test cases that attempts to avoid identified pitfalls with other frameworks reviewed, such as being overly complex to test for, or test cases that were too generalized to be uniformly applied. This proposed framework provides a tightly coupled set of test cases that map rather easily back to the data gathered during the assessment, limiting gaps in results, and providing more accurate conclusions than can often be derived with other frameworks. While not originally planned for in this dissertation's proposal, this proposed framework provides for one more dimension of analysis that may be helpful for future researchers to analyze with for their own samples when following a similar research methodology.
4. **Device Results Framework Mapping:** The heart of this dissertation's initial proposal was to provide analysis using existing IoT security frameworks to help discern whether real-world devices were living up to the types of controls noted within these publications. As such, a core contribution to the literature are the control mappings to the gathered meta data (see Appendices A, C, & E) and the results of those mappings to highlight where conditions resulted in a *Pass* or *Fail* against assessed frameworks from ETSI and DCMS (see Appendices D & F). In practice, any number of published frameworks could

have their controls mapped against the research's resultant data for device samples, however it was determined that two frameworks would be the goal for this research. This was ultimately supplemented by the proposed IoT framework published with this dissertation, leading to three distinctly different lenses for researchers to observe the overall meta data that was gathered about each of the research sample devices.

5. **Extracted Credentials:** Through the process of assessing the device sample, numerous credentials were identified through reading user manuals, accessing firmware images, and interacting with devices under operation. As observable in the enumerated list (see Appendix H) credentials on IoT devices may be the same – down to the cryptographic hash representation of the password. When such a hash is the same, an inference can be drawn by a researcher that the firmware may be similar (or the same) between devices, helping to provide further insight to supply chain commonality between samples. Further, the availability of credentials provides additional value in the literature as it can help researchers gain access to devices they may be trying to analyze. While credentials may be found on the internet, several credentials provided in this dissertation were unable to be identified as being known prior through usual (e.g., Github, Google) locations.

Research data sets, evidence, and artifacts that can be publicly published without potential liability for infringement on device vendor's intellectual property can be found at the following URL https://github.com/mstanislav/phd-dissertation, which provides a Git repository hosting the data. Exports of primary data sets will be provided in multiple formats (e.g., XLSX, CSV, JSON) to allow researchers easier access to apply the raw data into their own work.

Limitations

The research presented within this dissertation has several limitations that must be explicitly noted to help prevent drawing any erroneous interpretations based on the resultant data included, representations of that data by the author, or otherwise drawing inferences that could lead to the intended value of this research being taken out of appropriate context. While not every limitation can be enumerated outright, this section attempts to catalog some of the most impactful notes that will help the reader understand the research and its results more accurately.

1. The research sample has noted constraints in the survey sample population that helps to enable some consistency in the devices chosen, which inherently means that many cameras on the market, including popular offerings (e.g., Ring, Blink, Nest), were not assessed. This may lead some readers to infer these cameras were excluded on purpose, but the main deciding factor to that outcome was simply Amazon's listed date of sale, which excluded many devices for not being first available in the year 2020 on the site.
2. The research's *broad market analysis* framing led to the inclusion of five distinct camera device types so appropriate representation was given. Due to the noted sample constraints, this led to a disproportionate number of devices across the sample where "Security Cameras" (n=20) represented half of the total (n=40) and the remaining four market segments each had ~13% (n=5) of the overall sample. This limitation makes it difficult to compare smaller market segments to the larger, more generalized segment. This issue is further conflated by the lack of specificity some cameras have in what segment that are intending to be sold against, since a camera can of course be used for numerous purposes. A "Security Camera" could of course be used as a baby monitor in many cases, whereas a "Pet Feeder" is unlikely to be used as a doorbell in any practical

sense. This limitation is best mitigated when looking across the total sample size for a more robust sense of cameras within the market than a segment vs. segment view.

3. Because the sample cameras were purchased sight unseen from Amazon to limit bias beyond intended constraints, the ability to assess each device equally is difficult in some cases and impossible in others. The variance in vendor technologies means that while a lot of the resultant data from the sample devices has commonality, key elements led the research to exclude certain types of findings entirely due to a lack of applicability. The largest disparity stems from the vendor's choice to use a Linux-based distribution or Huawei's LiteOS for the system firmware. There are dramatic differences in how each OS is implemented, which led to many additional data elements to be collected for Linux-based devices, for instance. Data mapping to security frameworks therefore may represent a difference in security between devices that simply has more to do with an applicability of those control tests than any notable security differences in the device.
4. The association of research findings against different control frameworks is rarely a one-to-one relationship, meaning that multiple data elements are used to determine an outcome. The mappings themselves are a best effort as the framework can often be very general for the conditions that must be met, they are biased towards a singular OS (e.g., Linux), and/or the author(s) of those frameworks focus on a specific type of IoT device.
5. When research data was assessed against controls for DCMS (see Appendix F) and ETSI (see Appendix D) these mappings often involved multiple criteria to provide a *Pass* or *Fail* condition due to their complexity, not all of which can be asserted for each sample device. In cases where data is not present that can affirmatively *Fail* a device for the test criteria, the device will show a *Pass*. While the use of an *Unknown* could have been

applied in these cases, the sheer number of variables at play with these generic frameworks would lead to a non-trivial number of results to yield that condition, limiting the value of these mappings. When reviewing these results, readers should take more value in when devices have a *Fail* than a *Pass*, since the former case will be based on data that was gathered and the latter may have a lack of data as the cause of the *Pass*.

6. The decision to use Amazon to source devices means that some vendors in the market may not have been chosen due to a decision not to sell on the website, or stock for a given device may have been depleted when device selections were occurring, artificially excluding them due to a lack of inventory at the time purchases were made. The date listed on the site for when a device was first made available may also be a function of Amazon.com sales, rather than when a device was manufactured or made available in practice through a source like a vendor's own website prior to Amazon.
7. Because sample devices were chosen based on pre-determined research constraints and not ease-of-assessment, some devices were simply unable to be accessed in a uniform manner when compared to other devices in the sample. For instance, the Amcrest device has numerous missing data elements due to a lack of success at gaining firmware in the typical methods used for the broader sample devices. In these cases, readers are advised to carefully understand conclusions drawn about the security of a device with a more discerning lens for devices that are missing data to affirmatively draw a conclusion.
8. Sample devices chosen were selected to provide unique vendors, going as far as avoiding cameras that appeared similar even if the noted vendors were different. The reality of supply chains for IoT is that manufacturers may sell a device to vendors who will then add their own custom branding, but not change anything about the device other than a

label or name. There are circumstances (e.g., Anran & Jennov) where the physical device layout is different, but the core components and firmware are nearly identical. This means that while the sample has all unique vendors, there are cases where devices are effectively the same or contain major components (e.g., firmware) that lead to less than 40 *unique* devices in practice. This limitation is worth noting, but in practice many vendors will reuse components from original design manufactures (ODM) within all sorts of supply chains, so the lack of uniqueness does not change much about these findings.

9. While each device's analysis followed a similar methodology, the amount of time or effort on a given sample was not directly controlled. Some devices were simply easier to gain access to or had less to explore once accessed. The research goal in this regard was to achieve as much completeness of gathered data per camera, without spending so much time on a single device as to have diminishing returns for the overall n=40 sample. More time, technology, effort, and experience could lead to further data to be gathered in spots where no data currently exists in the research findings, but the practical ability to commit to each device until 100% complete is not within the timeline of this study.
10. Firmware updates, different code trains, model differences, and other variables about the assessed devices are unable to provide a true *vendor security* perspective. A single device per vendor may be informative about some aspects about their approach to engineering, security norms, or otherwise, but these results should not be taken as a vendor-specific conclusion as the assessed device may be one of many that is sold and could each have very different types of decisions made based on the product itself.

Future Research

This research study had a forward-looking hope that the data provided would be robust enough to allow other researchers to take the raw data and perform their own mappings against security frameworks – either custom or industry-provided. While mappings are provided against three frameworks, the literature review provides the reader awareness that many more frameworks exist today and reasonably, will continue to be created in the future. Researchers may also conclude that the approach to mapping this study's data to given frameworks were perhaps done differently than they would have chosen and may, therefore, be re-mapped later with an altered perspective, depth, or complexity within their process.

Future research in this area may also leverage the research approach to gather equivalent data about other IoT device segments, different vendors, different product lines, or just newer firmware versions of existing devices. In any case, researchers who follow this overall data framework can bring their own results and expand this initial sample to further provide the research community with an even more robust corpus of data to analyze as is beneficial for other types of studies.

As also described in the literature review, many researchers have taken a vulnerability-centric analysis of devices, looking for exploitable conditions that lead to compromise. This research study took much more of a meta-data centric approach to understanding security, providing robust insight into different aspects of a device that could provide security risk or resilience. It would therefore be worth exploring these results beyond this study's intention and identify specific security vulnerabilities in protocols, services, & configurations that could lead to attackers being able to abuse device functionality, whether local to the device or remotely.

Further analysis could also be conducted to confirm that implemented controls (e.g., cryptographic digital signature verification) are working as intended. While this overlaps with vulnerability analysis, the more direct goal would be to ensure that security features are adding intended resilience against attackers, rather than any attackable functionality itself. This could extend into topics like privacy analysis, validating that data deletion is robust (e.g., overwriting data, rather than simply unlinking inodes on the filesystem). The research conducted in many of these areas were presence-focused, rather than validating each control's effectiveness.

Lastly, future researchers would benefit the community by automating the data gathering, analysis, and indexing of the data found within this study. Much of the work was done quite manually and is difficult to scale in practice. However, a combination of tooling and scripting could, in many cases, extract quite a bit of this data either real-time (e.g., UART serial interface scripting) or at-rest (e.g., firmware analysis to extract conclusions). This sort of automation seems obvious on the surface, but the effort to script such data gathering when devices can be quite unique sample-to-sample can lead to data quality issues or overt complexity to do this well.

Summary

This research sought to establish a robust data set through technical analysis from a survey sample of 40 recent IoT cameras that span multiple market segments and map those findings against industry frameworks to establish a perspective on their multi-dimensional security integrity. This study was conducted through the creation of an assessment-tracking mechanism that uniformly indexed the findings of the technical analysis. Additionally, a proposed IoT security framework was created and used for an additional approach to determine the security composition of a given device within the survey's sample.

This study adds a robust, organized, granular data set for a significant sample of IoT devices that share common traits to provide for a controlled set of criteria with which to compare security findings more easily for. Researchers will be able to use this data to conduct their own analysis with other security frameworks, analyze the composition of devices in the market, and understand which devices may have attributes of value to their own research agendas. The framework mapping of the results set provides a variety of perspectives on how security can be determined for a given IoT device and its ecosystem. This analysis can be used to define relationships between security elements beyond those already included within this study.

Future research study ideas were shared to further the value of this research and encourage additional approaches to further maximize understanding the security elements of this research that were not addressed.

REFERENCES

Alharbi, R, & Aspinall, D. (2018). An IoT analysis framework: an investigation of IoT smart cameras' vulnerabilities. *Living in the Internet of things: cybersecurity of the IoT - 2018*, 47.

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. *Technologies*, *6*(3), 64. https://doi.org/10.3390/technologies6030064

Axis Communications. (2002). *AXIS 2100 network camera*. https://www.axis.com/files/datasheet/2100/2100_ds.pdf

Babbie, E. (2014). *The Basics of Social Research* (6th ed.). Belmont, CA: Cengage.

Bashis. (2004, August 25). *Axis network cameras let remote users view and edit files on the device*. SecurityTracker. https://securitytracker.com/id?1011056

Bell, K. (2020, January 13). *Ring hit with class action lawsuit for 'failure to take basic security precautions'*. Mashable. https://mashable.com/article/ring-class-action-lawsuit-hacking-security/

Biggs, J. (2014, November 7). *Insecam displays unsecured webcams from around the world*. TechCrunch. https://techcrunch.com/2014/11/07/insecam-displays-insecure-webcams-from-around-the-world/

Brice-Saddler, M., Selk, A., & Rosenberg, E. (2019, March 29). *Prankster sentenced to 20 years for fake 911 call that led police to kill an innocent man*. The Washington Post. https://www.washingtonpost.com/nation/2019/03/29/prankster-sentenced-years-fake-call-that-led-police-kill-an-innocent-man/

Bugeja, J., Jonsson, D., & Jacobsson, A. (2018). An investigation of vulnerabilities in smart connected cameras. *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*.

Bursztein, E. (2017, December 6). *Inside Mirai the infamous IoT botnet: A retrospective analysis*. Elie. https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

CamHacker. (2019, March 16). *Webcam FAQ*. https://www.camhacker.com/faq/

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020, May 29). Trust in the smart home: Findings from a nationally representative survey in the UK. *PloS One*, *15*(5), e0231615–e0231615. https://doi.org/10.1371/journal.pone.0231615

Carnegie Mellon University. (2017, August). *The CERT® Guide to Coordinated Vulnerability Disclosure*. Software Engineering Institute Digital Library. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Cisco. (2017). *The IoT value/trust paradox: building trust and value in the data exchange between people, things and providers*.

Cloud Security Alliance. (2019). *Guide to the CSA Internet of Things (IoT) security controls framework*. https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/

Console Cowboys. (2012, January 10). *Trendnet cameras - I always feel like somebody's watching me*. https://console-cowboys.blogspot.com/2012/01/trendnet-cameras-i-always-feel-like.html

Consumers International and Internet Society. (2018). *ConnectSmart! Smart products can enhance our lives, but there can also be risks* [Flyer]. Internet Society. https://www.internetsociety.org/wp-content/uploads/2018/11/ConnectSmart.pdf

Council to Secure the Digital Economy. (2019). *The C2 consensus on IoT device security baseline capabilities*. https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches.* Fourth edition. Los Angeles: SAGE.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: qualitative, quantitative, and mixed methods approaches.* Fifth edition. Los Angeles: SAGE.

CTIA. (2021, January 27). *Cybersecurity certification program for IoT devices*. https://ctiacertification.org/device-certification-programs/

CTIA Certification. (2018, October 3). *CTIA IoT cybersecurity certification program begins accepting devices for testing*. https://ctiacertification.org/news/ctia-iot-cybersecurity-certification-program-begins-accepting-devices-for-testing/

Davis, M. (2015). *Petcube remote wireless pet camera vulnerabilities*. IOActive. https://ioactive.com/wp-content/uploads/2018/05/IOActive_Advisory_Petcube.pdf

Doffman, Z. (2020, March 21). *Putin's secret intelligence agency hacked: dangerous new 'cyber weapons' now exposed*. Forbes. https://www.forbes.com/sites/zakdoffman/2020/03/21/putins-secret-intelligence-agency-hacked-dangerous-new-cyber-weapons-target-your-devices/

European Union Agency for Network and Information Security. (2017). *Baseline security recommendations for IoT in the context of Critical Information Infrastructures*. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

European Telecommunications Standards Institute. (2020, June). *Cyber Security for Consumer Internet of Things: Baseline Requirement*. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Federal Bureau of Investigation. (2020, December 29). *Recent swatting attacks targeting residents with camera and voice-capable smart devices*. Internet Crime Complaint Center. https://ic3.gov/Media/Y2020/PSA201229

Federal Trade Commission. (2014). *In the Matter of TRENDNET, INC., a corporation* (122 3090). https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf

Federal Trade Commission. (2014). *In the Matter of TRENDNET, INC., a corporation* (122 3090). https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf

Federal Trade Commission. (2016, October 28). *DMCA security research exemption for consumer devices*. https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices

Federal Trade Commission. (2017, January 5). *FTC charges D-link put consumers' privacy at risk due to the inadequate security of its computer routers and cameras*. https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate

Ferreira, B. (2017, January 22). *Hack a Furby to Rickroll your friends through its creepy eyeball menu*. VICE. https://www.vice.com/en/article/yp3jjx/furby-rickroll-hack

Fisher, D. (2014, February 18). *Researchers find serious flaws in WeMo home automation devices*. Threatpost. https://threatpost.com/researchers-find-serious-flaws-in-wemo-home-automation-devices/104300/

FOX19. (2014, July 2). *Hacker hijacks baby monitor*. https://www.fox19.com/story/25310628/hacked-baby-monitor/

Franceschi-Bicchierai, L. (2017, July 28). *More than 120,000 internet connected cameras can be easily hacked, researcher warns*. VICE. https://www.vice.com/en/article/j5qwb8/more-than-120000-internet-connected-cameras-can-be-easily-hacked-researcher-warns

Goodin, D. (2016, September 28). *Record-breaking DDoS reportedly delivered by >145k hacked cameras*. Ars Technica. https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Grand, J. (2004, August 6). *Practical secure hardware design for embedded systems (Part 1 of 2)*. InformIT. https://www.informit.com/articles/article.aspx?p=328170&seqNum=3

Grand View Research. (2019, September). *Smart baby monitor market size worth $1.7 billion by 2025*. https://www.grandviewresearch.com/press-release/global-smart-baby-monitor-market

Grand View Research. (2020, May). *Smart home security cameras market size report, 2020-2027*. https://www.grandviewresearch.com/industry-analysis/smart-home-security-camera-market

Greenberg, A. (2016, January 27). *NYC launches investigation into hackable baby monitors*. Wired. https://www.wired.com/2016/01/nyc-investigating-hackable-baby-monitors/

Greene, T. C. (2000, June 25). *Crackers use search engines to exploit weak sites*. The Register. https://www.theregister.com/2000/06/25/crackers_use_search_engines/

Guzman, A., & Bassem, C. (2021). *ISVS - IoT security verification standard* (v1.0-RC). Open Web Application Security Project. https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS/releases/download/1.0RC/OWASP_ISVS-1.0RC-en_WIP_.pdf

Harwood, T. (2019, November 12). *Internet of things (IoT) history*. Postscapes. Retrieved February 10, 2021, from https://www.postscapes.com/iot-history/

Help Net Security. (2017, January 5). *IoT trust framework: The foundation for future IoT certification programs*. https://www.helpnetsecurity.com/2017/01/05/iot-trust-framework/

Hill, K. (2013, August 13). *How a creep hacked a baby monitor to say lewd things to a 2-year-old*. Forbes. https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/

Hill, K. (2013, August 27). *'Baby monitor hack' could happen to 40,000 other Foscam users*. Forbes. https://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/

Hilt, S., Mercês, F., Rosario, M., & Sancho, D. (2020). *Worm war: The botnet battle for IoT territory*. Trend Micro. https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf

Holley, J. (2019, December 12). *Family says hackers accessed a ring camera in their 8-year-old daughter's room*. WMC5. https://www.wmcactionnews5.com/2019/12/11/family-says-hackers-accessed-ring-camera-their-year-old-daughters-room/

India Telecommunication Engineering Center. (2020). *Draft guidelines / code of practice for securing consumer Internet of Things (IoT)*. https://www.tec.gov.in/pdf/Whatsnew/Code%20of%20Practice_Consumer%20IoT.pdf

Ingram, M. (2015, July 23). *Baby monitor camera hacked while child rocked to sleep*. CTV News. https://london.ctvnews.ca/baby-monitor-camera-hacked-while-child-rocked-to-sleep-1.2483149

Insecam. (n.d.). *Live cameras directory*. Retrieved February 11, 2021, from https://insecam.org

International Organization for Standardization. (2018). *ISO/IEC 27000:2018*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:en

International Telecommunication Union. (2012). *Overview of the Internet of things* (ITU-T Y.2060). https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

International Telecommunication Union. (2015). *Smart home profiles for 6LoWPAN devices* (Supplement 57). https://www.itu.int/ITU-T/recommendations/rec.aspx?id=12577

Internet of Things Cybersecurity Improvement Act of 2020. (2020). https://www.congress.gov/bill/116th-congress/house-bill/1668/text

"Internet of Things" devices may bring cyber exploitation. (2017). Teller Vision, (1484), 4-5.

IoT Alliance Australia. (2017). *Internet of Things security guideline* (v1.2). https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

IoT Security Foundation. (2016). *IoT security compliance framework - release 1.0*. https://www.iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

IoT Security Foundation. (2020). *IoTSF issues update to popular IoT security compliance framework* (v2.1). https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework/

Jiang, W. (2015, April 21). *Baby monitor apps could give hackers a glimpse into your kid's bedroom*. CBS New York. https://newyork.cbslocal.com/2015/04/21/seen-at-11-cyber-spies-could-target-your-child-through-a-baby-monitor/

Kaye, E., & Midgett, J. (2019). *A framework of safety for the Internet of Things: considerations for consumer product safety*. U.S. Consumer Product Safety Commission. https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019_0.pdf

Krebs, B. (2016, September 21). *KrebsOnSecurity hit with record DDoS*. Krebs on Security. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Krebs, B. (2016, October 21). *Hacked cameras, DVRs powered today's massive internet outage — Krebs on security*. Krebs on Security. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Lanier, Z., & Stanislav, M. (2014, February). *The Internet of Things: we've got to chat* [Conference session]. BSides San Francisco 2014, San Francisco, California. https://speakerdeck.com/mstanislav/the-internet-of-things-weve-got-to-chat

Long, J. (2002). *googleDorks*. https:// johnny.ihackstuff.com/security/googleDorks.shtml

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology. *ACM Transactions on Management Information Systems*, *2*(2), 1-25. https://doi.org/10.1145/1985347.1985353

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (v1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Newman, P. (2020, March 6). *The Internet of things 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue*. Business Insider. https://www.businessinsider.com/internet-of-things-report

Notopoulos, K. (2012, February 3). *Somebody's watching: how a simple exploit lets strangers tap into private security cameras*. The Verge. https://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan

Online Trust Alliance. (2015, October 28). *OTA releases new Internet of things trust framework to address global consumer concerns*. Internet Society. https://www.internetsociety.org/news/press-releases/2015/ota-releases-new-internet-of-things-trust-framework-to-address-global-consumer-concerns/

Online Trust Alliance. (2016). *OTA IoT trust framework*. http://purplefrog.tistory.com/attachment/cfile25.uf@215D683658A3B6D11831C9.pdf

Online Trust Alliance. (2017). *OTA IoT trust framework* (v2.5). Internet Society. https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_EN.pdf

Paganini, P. (2016, January 3). *@FFD8FFDB Twitter bot spies on poorly configured cameras*. Security Affairs. https://securityaffairs.co/wordpress/43244/digital-id/ffd8ffdb-twitter-bot.html

Palmer, D. (2017, May 10). *120,000 IoT cameras vulnerable to new Persirai botnet say researchers*. ZDNet. https://www.zdnet.com/article/120000-iot-cameras-vulnerable-to-new-persirai-botnet-say-researchers/

Praetorian Labs. (2016, March 16). *Why are JTAG and UART still effective attack vectors for IoT devices?* Praetorian. https://www.praetorian.com/blog/why-are-jtag-and-uart-still-effective-attack-vectors-for-iot-devices/

Pride, W., Ferrell, O.C., Lukas, B.A., Schembri, S., Niininen, O. and Cassidy, R. (2018). *Marketing principles (*Third edition, p 200). Cengage.

Rascon, J., & Aragon, R. (2018, December 18). *Man hacks wireless baby monitor, makes vulgar threats to family*. KPRC. https://www.click2houston.com/news/2018/12/19/man-hacks-wireless-baby-monitor-makes-vulgar-threats-to-family/

Rawat, A. S. (2021, March 31). *What is descriptive analysis? - types and advantages*. Analytics Steps. https://www.analyticssteps.com/blogs/overview-descriptive-analysis

Rubenking, N. J. (2013, August 2). *Who's watching? Hacked security cams spoof images, attack network*. PCMag. https://www.pcmag.com/news/whos-watching-hacked-security-cams-spoof-images-attack-network

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, *32*(2), 344-354. https://doi.org/10.5465/amr.2007.24348410

Schwartz, J. (2002, April 14). Nanny-cam may leave a home exposed. *New York Times*. https://www.nytimes.com/2002/04/14/business/nanny-cam-may-leave-a-home-exposed.html

Singel, R. (2007, October 1). *Sneaky white hats pull surveillance cam Switcheroo*. Wired. https://www.wired.com/2007/10/sneaky-white-hats-pull-surveillance-cam-switcheroo/

Smith. (2014, November 6). *Peeping into 73,000 unsecured security cameras via default passwords*. CSO Online. https://www.csoonline.com/article/2844283/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html

Smith. (2016, November 20). *IoT security camera infected within 98 seconds of plugging it in*. CSO Online. https://www.csoonline.com/article/3143133/iot-security-camera-infected-within-98-seconds-of-plugging-it-in.html

Stanislav, M., & Beardsley, T. (2015). *Hacking IoT: A case study on baby monitor exposures and vulnerabilities*. Rapid7. https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

Sun, D. (2020, October 12). *Singapore home cams hacked and stolen footage sold on pornographic sites*. The New Paper. https://www.tnp.sg/news/singapore/hackers-hawk-explicit-videos-taken-spore-home-cams

The Internet of Things and consumer product hazards. (2018, March 27). Federal Register. https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards

Toor, A. (2013, January 22). *Creepstreams: An interactive map of insecure webcam feeds (update)*. The Verge. https://www.theverge.com/2013/1/22/3902698/trendnet-security-camera-streams-mapped-out

U.K. Department for Digital, Culture, Media & Sport. (2018). *Code of practice for consumer IoT security*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

UL. (2019). *UL MCV 1376: Methodology for marketing claim verification*. https://www.shopulstandards.com/ProductDetail.aspx?UniqueKey=35953

U.S. Copyright Office. (2015, October 28). *Exemption to prohibition on circumvention of copyright protection systems for access control technologies. Federal Register. https://www.federalregister.gov/documents/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control*

Vamosi, R. (2014, August 13). *Hard-coded credentials still haunt many legacy IoT products*. Forbes. https://www.forbes.com/sites/robertvamosi/2014/08/13/hard-coded-credentials-still-haunt-many-legacy-iot-products/

Whitehouse, O. (2014). *Security of things: An implementers' guide to cyber-security for Internet of Things devices and beyond*. NCC Group. https://research.nccgroup.com/wp-content/uploads/2020/07/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_internet_of_things_devices_and_beyond-2.pdf

Whittaker, Z. (2019, November 7). *Amazon ring doorbells exposed home Wi-Fi passwords to hackers*. TechCrunch. https://techcrunch.com/2019/11/07/amazon-ring-doorbells-wifi-hackers/

APPENDICES

APPENDIX A: PROPOSED IOT SECURITY FRAMEWORK

Hardware Integrity (HW)

HW-01: The device features internal enhancements (e.g., epoxy, glue, shielding) that would visibly indicate potential physical tampering of hardware components.

- **Control Test:** If the device can be physically interacted with (e.g., dump flash chip) by an attacker without obvious physical intrusion, the device has failed this control.

HW-02: The device features a design (e.g., glued shell) or enhancements (e.g., tamper-evident stickers) that would indicate potential physical tampering of hardware components.

- **Control Test:** If the device can be opened by an attacker to expose internal components and sealed again without obvious physical intrusion, the device has failed this control.

HW-03: The device has a unique identifier (e.g., serial number) that is provided by the vendor during manufacturing that is able to be referenced for core operations (e.g., bootstrapping).

- **Control Test:** If the device does not provide a unique identifier that allows for physical association to a specific unit, the device has failed this control.

HW-04: The device has an FCC certification process performed for wireless functionality (e.g., Wi-Fi, Bluetooth) which ensures it is compliant to use within the United States.

- **Control Test:** If the device does not provide (e.g., box, shell) an FCC identifier, and one cannot be found (e.g., FCC search), the device has failed this control.

HW-05: The device utilizes a flash memory package that is less easily accessible (e.g., BGA) to an attacker with existing internal device access.

- **Control Test:** If a device utilizes a flash package that is easily accessible to an attacker with existing internal device access (e.g., SOIC), the device has failed the control.

Local Access (LA)

LA-01: The device does not readily expose a UART that can readily provide a physical attacker with an ability to interact with the OS and/or bootloader of the device.

- **Control Test:** If the device exposes (e.g., pads, headers) a UART that could be accessed by an attacker to interact with the OS and/or bootloader, then the device has failed this control.

LA-02: The device, featuring a UART, does not provide an ability to interact with the bootloader in a manner that lets an attacker change bootloader without limitation (e.g., password).

- **Control Test:** If the device's UART provides access to a bootloader without mitigation that can allow for an attacker to manipulate settings, the device has failed this control.
- **Dependency:** LA-01

LA-03: The device, featuring a UART, does not provide an ability to login directly to the OS from that interface with credentials, if known or discoverable to the attacker.

- **Control Test:** If the device's UART provides a login interface that would allow an attacker to provide credentials to gain a shell on the system, the device has failed the control.
- **Dependency:** LA-01

LA-04: The device, featuring a UART, does not provide an automatic shell -- with no credentials provided -- that could be used by an attacker to directly interact with the OS.

- **Control Test:** If the device's UART provides a direct, unauthenticated system shell to an attacker, the device has failed the control.
- **Dependency:** LA-01

LA-05: The device, featuring a UART, does not provide output that contains sensitive information (e.g., Wi-Fi settings, cloud service tokens) about the device's configuration.

- **Control Test:** If the device's UART shows sensitive data that could be valuable to attacker from merely observing the UART's output, the device has failed the control.
- **Dependency:** LA-01

Mobile Security (MS)

MS-01: The device's associated mobile application protects sensitive data (e.g., Wi-Fi settings) in files and databases that are not cleartext (e.g., encrypted database strings).

- **Control Test:** If a device's mobile application stores sensitive data in a manner that allows an attacker to readily read its contents, the device has failed the control.

MS-02: The device's associated mobile application protects network connection (e.g., APIs) via a method (e.g., certificate pinning) that prevents an attacker from readily intercepting traffic.

- **Control Test:** If a device's mobile application can have its network connections intercepted on an attacker-controlled device with a proxy configuration, the device has failed the control.

MS-03: The device's associated mobile application provides notification (and/or prevents usage) if that mobile device has indications that it has been "rooted" or "jail broken."

- **Control Test:** If a device's mobile application can be rooted or jail broken without the end-user being notified (and/or prevented) prior to its usage, the device has failed the control.

MS-04: The device's associated mobile application provides a cloud service that enforces a well-defined password policy to limit insecure password selection by end-users.

- **Control Test:** If a device's mobile application does not enforce a well-defined password policy requirement with its related cloud service, the device has failed the control.

MS-05: The device's associated mobile application provides a cloud service that supports a second step of authentication, beyond only a password.

- **Control Test:** If a device's mobile application does not allow an end-user to configure a second step of authentication with its related cloud service, the device has failed the control.

MS-06: The device's associated mobile application provides a cloud service that requires a second step of authentication, beyond only a password.

- **Control Test:** If a device's mobile application does not require an end-user to configure a second step of authentication with its related cloud service, the device has failed the control.
- **Dependency:** MS-05

MS-07: The device's associated mobile application uses encrypted traffic (e.g., HTTPS) for API calls or similar network connectivity with any associated cloud services.

- **Control Test:** If a device's mobile application does not use encrypted transports for APIs or similar network connectivity with cloud services, the device has failed the control.

Wi-Fi Security (WF)

WF-01: The device's configuration of Wi-Fi for use in an end-user's network does not allow the usage of Wi-Fi Protected Setup (WPS) due to known security design flaws in the protocol.

- **Control Test:** If a device supports the usage of WPS to configure Wi-Fi for connecting to an end-user's network, the device has failed the control.

WF-02: The device's configuration of Wi-Fi allows the use of Wi-Fi Protected Access 3 (WPA 3) when the relevant network supports the protocol itself.

- **Control Test:** If a device does not support the use of WPA 3 to connect to an end-user's network that supports the WPA 3 protocol, the device has failed the control.

WF-03: The device's configuration of Wi-Fi for use in an end-user's network does not allow a temporary Wi-Fi network to be created on the device, limiting potential attack surface.

- **Control Test:** If a device allows the creation of a temporary Wi-Fi network to connect to an end-user's network as a supported setup option, the device has failed the control.

WF-04: The device, supporting a temporary Wi-Fi network for configuration, requires a password to connect to that temporary network for the setup process to occur.

- **Control Test:** If a device, supporting a temporary Wi-Fi network for configuration, does not require a password to connect to that network, the device has failed the control.
- **Dependency:** WF-03

Service Security (SS)

SS-01: The device does not run a hosted web server that is network accessible (beyond localhost) that may support device management, streaming, or other features.

- **Control Test:** If a device hosts a local web server that is network accessible, the device has failed the control.

SS-02: The device, running a local web server that is network accessible, uses only encrypted transports (e.g., HTTPS) to handle all inbound traffic to its functionality.

- **Control Test:** If a device, running a local web server that is network accessible, does not encrypt traffic for its functionality, the device has failed the control.
- **Dependency:** SS-01

SS-03: The device, running a local web server that is network accessible, performs an authentication process before commands will be allowed to service endpoints.

- **Control Test:** If a device, running a local web server that is network accessible, does not require authentication before commands are allowed, the device has failed the control.
- **Dependency:** SS-01

SS-04: The device is not running a File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), or other inbound file transfer service during its normal operation.

- **Control Test:** If a device is running an inbound file transfer service during its normal operation, the device has failed the control.

SS-05: The device is not running a Secure Shell (SSH), Telnet, or other inbound remote access service during its normal operation.

- **Control Test:** If a device is running an inbound remote access service during its normal operation, the device has failed the control.

SS-06: The device is not running a local streaming service (e.g., RTSP) in its default configuration (i.e. without explicit user permission).

- **Control Test:** If a device is running a local streaming service in its default configuration, the device has failed the control.

SS-07: The device, running a local streaming service, encrypts the transmission of all video and/or audio.

- **Control Test:** If a device, running a local streaming service, does not encrypt all video and/or audio, the device has failed the control.
- **Dependency:** SS-06

SS-08: The device, running a local streaming service, requires authentication to access video and/or audio.

- **Control Test:** If a device, running a local streaming service, does not require authentication before video and/or audio can be accessed, the device has failed the control.
- **Dependency:** SS-06

SS-09: The device implements a host-based firewall (e.g., iptables) to limit ingress and/or egress traffic.

- **Control Test:** If a device does not implement a host-based firewall to limit ingress and/or egress traffic, the device has failed the control.

SS-10: The device is configured to prevent automatic IP forwarding from one network interface to another.

- **Control Test:** If a device has IP forwarding enabled, the device has failed the control.

SS-11: The device, leveraging MQ Telemetry Transport (MQTT) for its operation, encrypts the transmission of all messages between the device and the external MQTT service.

- **Control Test:** If a device, leveraging MQTT service for its operation, does not encrypt transmissions between the device and the external service, the device has failed the control.

Hardware Security (HS)

HS-01: The device's hardware supports Secure Boot as part of its shipped components (e.g., SoC).

- **Control Test:** If a device's hardware does not provide support for Secure Boot functionality, the device has failed the control.

HS-02: The device's hardware, supporting Secure Boot functionality, uses that as part of standard operation.

- **Control Test:** If a device's hardware, supporting Secure Boot functionality, does not leverage that as part of standard operation, the device has failed the control.
- **Dependency:** HS-01

HS-03: The device's hardware supports cryptographic operations via a provided security engine as part of its shipped components (e.g., SoC).

- **Control Test:** If a device's hardware does not provide a security engine that supports cryptographic operations, the device has failed the control.

HS-04: The device's hardware supports random number generation operations via a provided security engine as part of its shipped components (e.g., SoC).

- **Control Test:** If a device's hardware does not provide a security engine that supports random number generation operations, the device has failed the control.

Firmware Updates (FW)

FW-01: The device supports a documented approach for end-users and/or the vendor to update the running firmware on the device.

- **Control Test:** If a device's firmware is unable to be updated through a documented approach by end-users and/or the vendor, the device has failed the control.

FW-02: The device, supporting a documented approach to update firmware, notifies the end-user that a new firmware update is available when using the associated mobile application.

- **Control Test:** If a device, supporting a documented approach to firmware updates, does not notify an end-user when a new firmware update is available, the device has failed the control.
- **Dependency:** FW-01

FW-03: The device, supporting a documented approach to update firmware, requires new firmware to be installed before the device can be used by the end-user.

- **Control Test:** If a device, supporting a documented approach to firmware updates, does not require new firmware updates to be installed before use, the device has failed the control.
- **Dependency:** FW-01

FW-04: The device, supporting a documented approach to update firmware, allows an end-user to request checking for new firmware updates in the associated mobile application.

- **Control Test:** If a device, supporting a documented approach to firmware updates, does not allow an end-user to check for firmware updates, the device has failed the control.
- **Dependency:** FW-01

FW-05: The device, supporting a documented approach to update firmware, transports that firmware via an encrypted transport (e.g., HTTPS), even if the firmware is encrypted itself.

- **Control Test:** If a device, supporting a documented approach to firmware updates, does not transport firmware updates via an encrypted transport, the device has failed the control.
- **Dependency:** FW-01

FW-06: The device, supporting a documented approach to update firmware, does not provide a direct method for an end-user to upload their own firmware image.

- **Control Test:** If a device, supporting a documented approach to firmware updates, provides a direct method for an end-user to upload firmware, the device has failed the control.
- **Dependency:** FW-01

FW-07: The device, supporting a documented approach to update firmware, performs a validation that transmitted firmware matches an expected cryptographic hash before installation.

- **Control Test:** If a device, supporting a documented approach to firmware updates, installs transmitted firmware without verifying a cryptographic hash, the device has failed the control.
- **Dependency:** FW-01

FW-08: The device, supporting a documented approach to update firmware, performs a digital signature verification tied to the vendor for a transmitted firmware image before installation.

- **Control Test:** If a device, supporting a documented approach to firmware updates, installs a transmitted firmware image without verifying a signature, the device has failed the control.
- **Dependency:** FW-01

End-user Privacy (EP)

EP-01: The device provides a documented method to physically reset the system to a factory-default state, suitable for re-configuration by a new owner (or disposal).

- **Control Test:** If a device does not provide a documented, physical method to perform a factory-reset of the system, the device has failed the control.

EP-02: The device, when performing a documented method to physically reset the system to a factory-default state, removes all sensitive data (e.g., Wi-Fi configuration) from the device.

- **Control Test:** If a device, when performing a vendor-documented method to physically reset the system, does not delete all sensitive data, the device has failed the control.
- **Dependency:** EP-01

EP-03: The device, when supporting external media (e.g., Micro SD) and performing a documented method to physically reset the device to a default state, deletes all files from the media.

- **Control Test:** If a device, performing a documented method to physically reset the system, does not delete all files from external media, the device has failed the control.
- **Dependency:** EP-01

EP-04: The device, when supporting external media (e.g., Micro SD), performs a method of obfuscation or encryption that limits casual viewing of recordings stored on the external media.

- **Control Test:** If a device, supporting external media, does not prevent casual viewing of the recordings on that media, the device has failed the control.

EP-05: The device provides a physical indication (e.g., illuminated LED) that the camera is currently streaming video to a mobile application or a direct method (e.g., RTSP).

- **Control Test:** If a device does not provide a physical indication that a video stream is occurring when accessed with a supported method, the device has failed the control.

EP-06: The device's filesystem is encrypted-at-rest in a manner that prevents an attacker with physical access to its flash memory from recovering the contents of that device.

- **Control Test:** If a device does not encrypt its filesystem in a manner that prevents an attacker with physical access from recovering its contents, the device has failed the control.

Binary Hardening (BH)

BH-01: The device has implemented at least partial Relocation Read-Only (RELRO), determined by evaluating a relevant system binary as a representitive sample.

- **Control Test:** If a device has not implemented at least partial RELRO, determined by evaluating a relevant system binary, the device has failed the control.

BH-02: The device has implemented stack canaries, determined by evaluating a relevant system binary as a representitive sample.

- **Control Test:** If a device has not implemented stack canaries, determined by evaluating a relevant system binary, the device has failed the control.

BH-03: The device has implemented a non-executable (NX) memory regions, determined by evaluating a relevant system binary as a representitive sample.

- **Control Test:** If a device has not implemented NX memory regions, determined by evaluating a relevant system binary, the device has failed the control.

BH-04: The device has implemented Position Independent Executables (PIE), determined by evaluating a relevant system binary as a representitive sample.

- **Control Test:** If a device has not implemented PIE, determined by evaluating a relevant system binary, the device has failed the control.

BH-05: The device has removed debugging symbols, determined by evaluating a relevant system binary as a representitive sample.

- **Control Test:** If a device has not removed debugging symbols, determined by evaluating a relevant system binary, the device has failed the control.

BH-06: The device has implemented Fortify Source, determined by evaluating a relevant system binary as a representitive sample.

- **Control Test:** If a device has not implemented Fortify Source, determined by evaluating a relevant system binary, the device has failed the control.

Linux Hardening (LH)

LH-01: The device has implemented control groups (cgroups) for at least some contexts.

- **Control Test:** If the device does not implement cgroups for at least some contexts, the device has failed this control.

LH-02: The device has implemented seccomp-bpf in a manner that adds protection to core system services.

- **Control Test:** If the device does not implement seccomp-bpf in a manner that adds protection to core system services, the device has failed the control.

LH-03: The device has implemented mandatory access controls (MAC) (e.g., SELinux, AppAromor) in a manner that adds protection to core system services.

- **Control Test:** If the device does not implement MAC in a manner that adds protection to core system services, the device has failed the control.

LH-04: The device has appropriately configured discetionary access controls (DAC) in a manner that limits file access to specific system services and users (e.g., not over-using root).

- **Control Test:** If the device does not implement DAC in a manner that limits file access to specific system services and users, the device has failed the control.

LH-05: The device generally executes system processes and services in a manner that leverages users with less privilege than root, either directly or via privilege separation.

- **Control Test:** If the device does not generally execute system processes and services in a manner that leverages users with less privilege than root, the device has failed the control.

LH-06: The device does not contain OS-level account passwords either in a default or hardcoded form, including blank passwords.

- **Control Test:** If the device contains OS-level account passwords either in a default or hardcoded form, including blank passwords, the device has failed the control.

LH-07: The device, if it contains OS-level account passwords either in a default or hardcoded form, store those passwords in a format other than md5crypt or descrypt.

- **Control Test:** If the device, containing OS-level account passwords, stores those passwords with md5crypt or descrypt, the device has failed the control.
- **Dependency:** LH-06

LH-08: The device's installed kernel is built from an actively maintained code train.

- **Control Test:** If the device has a kernel that is built from an unmaintained code train, the device has failed the control.

LH-09: The device's installed kernel modules supporting core functionality are digitally signed.

- **Control Test:** If the device has kernel modules providing core functionality that are not digitally signed, the device has failed the control.

LH-10: The device has at least partial enablement for Address Space Layout Randomization (ASLR).

- **Control Test:** If the device does not have at least partial ASLR enabled, the device has failed the control.

APPENDIX B: PROPOSED IOT SECURITY FRAMEWORK – CAMERA MAPPING

Baby Monitors

CellBee

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Pass				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	0/7 0%	6/7 86%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Fail				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	4/11 36%	2/11 18%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Pass				
	SS-07	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
Hardware Security (HW)	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	4/8 50%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Pass				
	FW-04	Fail				
	FW-05	Pass				
	FW-06	Fail				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Pass	3/10 30%	7/10 70%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Pass				
	LH-08	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		22/66 33%	37/66 56%	0/66 0%	7/66 11%
			Pass	**Fail**	**Unknown**	**N/A**

Kami Baby

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Pass				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	2/7 29%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	4/4 100%	0/4 0%	0/4 0%	0/4 0%
	HW-02	Pass				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	2/8 25%	2/8 25%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	2/10 20%	8/10 80%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Pass				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		30/66 45%	26/66 39%	2/66 3%	8/66 12%
			Pass	**Fail**	**Unknown**	**N/A**

Motorola

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Pass				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	2/7 29%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	5/11 45%	4/11 36%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Fail				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	6/8 75%	2/8 25%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Pass				
	FW-04	Pass				
	FW-05	Pass				
	FW-06	Fail				
	FW-07	Pass				
	FW-08	Pass				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	1/6 17%	0/6 0%	2/6 33%
	EP-02	Pass				
	EP-03	N/A				
	EP-04	N/A				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	0/6 0%	6/6 100%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Fail				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	7/10 70%	3/10 30%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Unknown				
	LH-07	Unknown				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		29/66 44%	28/66 42%	3/66 5%	6/66 9%
			Pass	**Fail**	**Unknown**	**N/A**

Sense-U

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	1/7 14%	5/7 71%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Fail	0/4 0%	3/4 75%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Fail				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Fail	0/8 0%	1/8 13%	0/8 0%	7/8 87%
	FW-02	N/A				
	FW-03	N/A				
	FW-04	N/A				
	FW-05	N/A				
	FW-06	N/A				
	FW-07	N/A				
	FW-08	N/A				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	9/10 90%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		16/66 24%	35/66 53%	4/66 6%	11/66 17%
			Pass	**Fail**	**Unknown**	**N/A**

VTech

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Pass				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	2/7 29%	3/7 43%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	6/8 75%	2/8 25%	0/8 0%	0/8 0%
	FW-02	Pass				
	FW-03	Pass				
	FW-04	Fail				
	FW-05	Pass				
	FW-06	Pass				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	2/6 33%	0/6 0%	2/6 33%
	EP-02	Fail				
	EP-03	N/A				
	EP-04	N/A				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		30/66 45%	26/66 39%	1/66 2%	9/66 14%
			Pass	**Fail**	**Unknown**	**N/A**

Doorbells

Energizer

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	5/7 71%	2/7 29%	0/7 0%	0/7 0%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Pass				
	MS-06	Fail				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	6/11 55%	3/11 27%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				

Category	ID	Status	Pass	Fail	Unknown	N/A
	SS-11	Pass				
Hardware Security (HW)	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	1/8 13%	3/8 38%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	4/6 67%	2/6 33%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	9/10 90%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
	Grand Total		32/66 48%	27/66 41%	4/66 6%	3/66 5%
			Pass	**Fail**	**Unknown**	**N/A**

Euarne

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	1/7 14%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	2/8 25%	1/8 13%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Fail				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		20/66 30%	16/66 24%	6/66 9%	24/66 36%
			Pass	**Fail**	**Unknown**	**N/A**

Eufy

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	3/7 43%	4/7 57%	0/7 0%	0/7 0%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Pass				
	MS-06	Fail				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	5/8 63%	3/8 38%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Pass				
	FW-04	Pass				
	FW-05	Pass				
	FW-06	Pass				
	FW-07	Fail				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	2/6 33%	1/6 17%	0/6 0%
	EP-02	Unknown				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		26/66 39%	16/66 24%	2/66 3%	22/66 33%
			Pass	**Fail**	**Unknown**	**N/A**

Victure

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	4/5 80%	1/5 20%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	2/7 29%	4/7 57%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	5/11 45%	4/11 36%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Fail				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	2/8 25%	1/8 13%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Fail				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		23/66 35% **Pass**	17/66 26% **Fail**	6/66 9% **Unknown**	20/66 30% **N/A**

Wuuk

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	3/7 43%	4/7 57%	0/7 0%	0/7 0%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Pass				
	MS-06	Fail				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	2/11 18%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Fail				
	SS-11	Pass				
	HW-01	Fail	1/4 25%	2/4 50%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	1/8 13%	3/8 38%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		23/66 35%	34/66 52%	3/66 5%	6/66 9%
			Pass	**Fail**	**Unknown**	**N/A**

Hidden Cameras

Camakt

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	4/5 80%	1/5 20%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	1/7 14%	5/7 71%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				

Category	ID	Status	Pass	Fail	Unknown	N/A
	SS-11	N/A				
Hardware Security (HW)	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	1/8 13%	3/8 38%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	1/6 17%	3/6 50%	2/6 33%	0/6 0%
	EP-02	Unknown				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Unknown				
Binary Hardening (BH)	BH-01	Unknown	0/6 0%	0/6 0%	6/6 100%	0/6 0%
	BH-02	Unknown				
	BH-03	Unknown				
	BH-04	Unknown				
	BH-05	Unknown				
	BH-06	Unknown				
Linux Hardening (LH)	LH-01	Unknown	0/10 0%	1/10 10%	9/10 90%	0/10 0%
	LH-02	Unknown				
	LH-03	Unknown				
	LH-04	Unknown				
	LH-05	Unknown				
	LH-06	Unknown				
	LH-07	Unknown				
	LH-08	Fail				
	LH-09	Unknown				
	LH-10	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
	Grand Total		19/66 29%	21/66 32%	20/66 30%	6/66 9%
			Pass	**Fail**	**Unknown**	**N/A**

Ecwey

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Pass				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	1/7 14%	3/7 43%	1/7 14%	2/7 29%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Fail	0/4 0%	4/4 100%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Fail	3/11 27%	5/11 45%	0/11 0%	3/11 27%
	SS-02	Fail				
	SS-03	Fail				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	1/8 13%	2/8 25%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Fail				
	FW-05	Unknown				
	FW-06	Fail				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		14/66 21%	40/66 61%	6/66 9%	6/66 9%
			Pass	**Fail**	**Unknown**	**N/A**

Pambrum

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	1/7 14%	4/7 57%	0/7 0%	2/7 29%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Pass	3/11 27%	3/11 27%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Fail				
	SS-05	Fail				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Fail	0/8 0%	1/8 13%	0/8 0%	7/8 87%
	FW-02	N/A				
	FW-03	N/A				
	FW-04	N/A				
	FW-05	N/A				
	FW-06	N/A				
	FW-07	N/A				
	FW-08	N/A				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Pass				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		15/66 23%	37/66 56%	3/66 5%	11/66 17%
			Pass	**Fail**	**Unknown**	**N/A**

Swept Supplies

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	4/5 80%	1/5 20%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	1/7 14%	4/7 57%	0/7 0%	2/7 29%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Pass	4/11 36%	2/11 18%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Fail	0/8 0%	1/8 13%	0/8 0%	7/8 87%
	FW-02	N/A				
	FW-03	N/A				
	FW-04	N/A				
	FW-05	N/A				
	FW-06	N/A				
	FW-07	N/A				
	FW-08	N/A				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Pass	1/10 10%	6/10 60%	3/10 30%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Unknown				
	LH-07	Unknown				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		16/66 24%	32/66 48%	6/66 9%	12/66 18%
			Pass	**Fail**	**Unknown**	**N/A**

VicZone

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Pass	3/7 43%	1/7 14%	1/7 14%	2/7 29%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Fail	3/11 27%	7/11 64%	0/11 0%	1/11 9%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Fail				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Fail	0/8 0%	1/8 13%	0/8 0%	7/8 87%
	FW-02	N/A				
	FW-03	N/A				
	FW-04	N/A				
	FW-05	N/A				
	FW-06	N/A				
	FW-07	N/A				
	FW-08	N/A				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		16/66 24%	38/66 58%	4/66 6%	8/66 12%
			Pass	**Fail**	**Unknown**	**N/A**

Pet Feeders

Didog

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	1/7 14%	5/7 71%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Pass	4/11 36%	2/11 18%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				

Category	ID	Status	Pass	Fail	Unknown	N/A
	SS-11	N/A				
Hardware Security (HW)	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				
	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	5/8 63%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Pass				
	FW-04	Fail				
	FW-05	Fail				
	FW-06	Fail				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	1/6 17%	0/6 0%	2/6 33%
	EP-02	Pass				
	EP-03	N/A				
	EP-04	N/A				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				

Category	ID	Status	Pass	Fail	Unknown	N/A
	Grand Total		19/66 29%	38/66 58%	0/66 0%	9/66 14%
			Pass	**Fail**	**Unknown**	**N/A**

HONGSA

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	1/7 14%	4/7 57%	0/7 0%	2/7 29%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Pass	3/11 27%	3/11 27%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Fail				
	SS-05	Fail				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	4/8 50%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	9/10 90%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		19/66 29%	39/66 59%	1/66 2%	7/66 11%
			Pass	**Fail**	**Unknown**	**N/A**

IOIODOG

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Pass	4/7 57%	1/7 14%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	0/4 0%	3/4 75%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Fail				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	0/8 0%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	4/6 67%	2/6 33%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		21/66 32%	31/66 47%	6/66 9%	8/66 12%
			Pass	**Fail**	**Unknown**	**N/A**

iSmartPet

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	0/7 0%	6/7 86%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Fail				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	3/11 27%	5/11 45%	0/11 0%	3/11 27%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Fail				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Fail	0/8 0%	1/8 13%	0/8 0%	7/8 87%
	FW-02	N/A				
	FW-03	N/A				
	FW-04	N/A				
	FW-05	N/A				
	FW-06	N/A				
	FW-07	N/A				
	FW-08	N/A				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	2/6 33%	0/6 0%	2/6 33%
	EP-02	Pass				
	EP-03	N/A				
	EP-04	N/A				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Pass	3/10 30%	7/10 70%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Pass				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		16/66 24%	35/66 53%	3/66 5%	12/66 18%
			Pass	**Fail**	**Unknown**	**N/A**

Sekoya

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	2/7 29%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Pass	3/11 27%	5/11 45%	1/11 9%	2/11 18%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Fail				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Fail				
	SS-09	Fail				
	SS-10	Unknown				
	SS-11	Pass				
	HW-01	Fail	1/4 25%	2/4 50%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	0/8 0%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Pass	1/10 10%	8/10 80%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		21/66 32%	34/66 52%	7/66 11%	4/66 6%
			Pass	**Fail**	**Unknown**	**N/A**

Security Cameras

Akaso

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	4/5 80%	1/5 20%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	1/7 14%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	5/11 45%	4/11 36%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Fail				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				

Category	ID	Status	Pass	Fail	Unknown	N/A
	SS-11	Pass				
Hardware Security (HW)	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				
	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	1/8 13%	3/8 38%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	4/6 67%	1/6 17%	1/6 17%	0/6 0%
	EP-02	Unknown				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Pass				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
	Grand Total		27/66 41%	13/66 20%	6/66 9%	20/66 30%
			Pass	**Fail**	**Unknown**	**N/A**

Amcrest

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Pass				
Local Access (LA)	LA-01	Fail	4/5 80%	1/5 20%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	2/7 29%	3/7 43%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Fail	4/11 36%	4/11 36%	2/11 18%	1/11 9%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Pass				
	SS-09	Unknown				
	SS-10	Unknown				
	SS-11	N/A				
	HW-01	Unknown	0/4 0%	0/4 0%	4/4 100%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Unknown				
	HW-04	Unknown				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	0/8 0%	4/8 50%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Pass				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	3/6 50%	1/6 17%	0/6 0%
	EP-02	Unknown				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Unknown	0/6 0%	0/6 0%	6/6 100%	0/6 0%
	BH-02	Unknown				
	BH-03	Unknown				
	BH-04	Unknown				
	BH-05	Unknown				
	BH-06	Unknown				
Linux Hardening (LH)	LH-01	Unknown	0/10 0%	1/10 10%	9/10 90%	0/10 0%
	LH-02	Unknown				
	LH-03	Unknown				
	LH-04	Unknown				
	LH-05	Unknown				
	LH-06	Unknown				
	LH-07	Unknown				
	LH-08	Fail				
	LH-09	Unknown				
	LH-10	Unknown				
	Grand Total		20/66 30%	17/66 26%	27/66 41%	2/66 3%
			Pass	**Fail**	**Unknown**	**N/A**

Anbes

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Pass				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	4/5 80%	1/5 20%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	2/7 29%	4/7 57%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	5/11 45%	4/11 36%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Fail				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	2/8 25%	1/8 13%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Fail				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	4/6 67%	2/6 33%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		25/66 38%	15/66 23%	6/66 9%	20/66 30%
			Pass	**Fail**	**Unknown**	**N/A**

Anran

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	1/7 14%	3/7 43%	1/7 14%	2/7 29%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	2/4 50%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Pass				
Service Security (SS)	SS-01	Fail	4/11 36%	6/11 55%	0/11 0%	1/11 9%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Fail				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	1/8 13%	4/8 50%	3/8 38%	0/8 0%
	FW-02	Fail				
	FW-03	Fail				
	FW-04	Fail				
	FW-05	Unknown				
	FW-06	Fail				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	4/6 67%	2/6 33%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		21/66 32%	38/66 58%	4/66 6%	3/66 5%
			Pass	**Fail**	**Unknown**	**N/A**

Aqara

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	1/7 14%	5/7 71%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	5/11 45%	4/11 36%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Fail				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	6/8 75%	2/8 25%	0/8 0%	0/8 0%
	FW-02	Pass				
	FW-03	Pass				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Pass				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	9/10 90%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		26/66 39%	35/66 53%	1/66 2%	4/66 6%
			Pass	**Fail**	**Unknown**	**N/A**

Conico

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	Pass				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	2/7 29%	4/7 57%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Fail	5/11 45%	4/11 36%	0/11 0%	2/11 18%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Fail				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	4/8 50%	0/8 0%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Fail				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		23/66 35% **Pass**	23/66 35% **Fail**	1/66 2% **Unknown**	19/66 29% **N/A**

DCT

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	N/A				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	2/7 29%	4/7 57%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	5/8 63%	0/8 0%	3/8 38%	0/8 0%
	FW-02	Pass				
	FW-03	Pass				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		22/66 33%	17/66 26%	4/66 6%	23/66 35%
			Pass	**Fail**	**Unknown**	**N/A**

Ecobee

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Pass				
Local Access (LA)	LA-01	Pass	1/5 20%	0/5 0%	0/5 0%	4/5 80%
	LA-02	N/A				
	LA-03	N/A				
	LA-04	N/A				
	LA-05	N/A				
Mobile Security (MS)	MS-01	Fail	4/7 57%	3/7 43%	0/7 0%	0/7 0%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Pass				
	MS-06	Pass				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Fail	5/11 45%	3/11 27%	0/11 0%	3/11 27%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	6/8 75%	1/8 13%	1/8 13%	0/8 0%
	FW-02	Pass				
	FW-03	Pass				
	FW-04	Pass				
	FW-05	Pass				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	1/6 17%	1/6 17%	2/6 33%
	EP-02	Unknown				
	EP-03	N/A				
	EP-04	N/A				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Fail				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	2/10 20%	6/10 60%	1/10 10%	1/10 10%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Pass				
	LH-07	N/A				
	LH-08	Pass				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		30/66 45%	21/66 32%	4/66 6%	11/66 17%
			Pass	**Fail**	**Unknown**	**N/A**

Eversecu

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Pass				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	1/7 14%	5/7 71%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	2/4 50%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Pass				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	0/8 0%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		17/66 26%	20/66 30%	6/66 9%	23/66 35%
			Pass	**Fail**	**Unknown**	**N/A**

Feit Electric

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	1/5 20%	0/5 0%	1/5 20%
	LA-02	Pass				
	LA-03	Pass				
	LA-04	N/A				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	2/7 29%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	1/8 13%	3/8 38%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	8/10 80%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Pass				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		30/66 45%	25/66 38%	4/66 6%	7/66 11%
			Pass	**Fail**	**Unknown**	**N/A**

HeimVision

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	LA-02	Fail				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	2/7 29%	3/7 43%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Fail	4/11 36%	6/11 55%	0/11 0%	1/11 9%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Fail				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	1/4 25%	2/4 50%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Pass	5/8 63%	1/8 13%	2/8 25%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Pass				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Fail				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		20/66 30%	40/66 61%	3/66 5%	3/66 5%
			Pass	**Fail**	**Unknown**	**N/A**

Jennov

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	LA-02	Pass				
	LA-03	Fail				
	LA-04	Pass				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	1/7 14%	3/7 43%	1/7 14%	2/7 29%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	N/A				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	2/4 50%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Pass				
Service Security (SS)	SS-01	Fail	4/11 36%	6/11 55%	0/11 0%	1/11 9%
	SS-02	Fail				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Fail				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Fail	0/8 0%	1/8 13%	0/8 0%	7/8 87%
	FW-02	N/A				
	FW-03	N/A				
	FW-04	N/A				
	FW-05	N/A				
	FW-06	N/A				
	FW-07	N/A				
	FW-08	N/A				
End-user Privacy (EP)	EP-01	Fail	0/6 0%	6/6 100%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	4/6 67%	2/6 33%	0/6 0%	0/6 0%
	BH-02	Pass				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		18/66 27%	37/66 56%	4/66 6%	7/66 11%
			Pass	**Fail**	**Unknown**	**N/A**

LaView

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Pass	1/5 20%	0/5 0%	0/5 0%	4/5 80%
	LA-02	N/A				
	LA-03	N/A				
	LA-04	N/A				
	LA-05	N/A				
Mobile Security (MS)	MS-01	Pass	4/7 57%	2/7 29%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Fail	0/4 0%	3/4 75%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Fail				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	0/8 0%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	4/6 67%	0/6 0%	0/6 0%
	EP-02	Fail				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	9/10 90%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		21/66 32%	28/66 42%	6/66 9%	11/66 17%
			Pass	**Fail**	**Unknown**	**N/A**

Mascarry

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	3/5 60%	2/5 40%	0/5 0%	0/5 0%
	HW-02	Pass				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Pass	1/5 20%	0/5 0%	0/5 0%	4/5 80%
	LA-02	N/A				
	LA-03	N/A				
	LA-04	N/A				
	LA-05	N/A				
Mobile Security (MS)	MS-01	Fail	1/7 14%	5/7 71%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	2/11 18%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Fail				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	2/8 25%	2/8 25%	0/8 0%
	FW-02	Pass				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	0/10 0%	9/10 90%	1/10 10%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Unknown				
	Grand Total		22/66 33%	30/66 45%	3/66 5%	11/66 17%
			Pass	**Fail**	**Unknown**	**N/A**

Moonxiao

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	0/5 0%	5/5 100%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	0/5 0%	4/5 80%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Fail	2/7 29%	4/7 57%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	3/11 27%	0/11 0%	3/11 27%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Fail				
	SS-07	Fail				
	SS-08	Pass				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Fail	0/4 0%	3/4 75%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Fail				
	HW-04	Fail				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	4/8 50%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Pass				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Fail				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Fail	1/6 17%	5/6 83%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Fail				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		18/66 27%	41/66 62%	0/66 0%	7/66 11%
			Pass	**Fail**	**Unknown**	**N/A**

Reolink

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	2/5 40%	2/5 40%	0/5 0%	1/5 20%
	LA-02	Pass				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	2/7 29%	4/7 57%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	2/8 25%	6/8 75%	0/8 0%	0/8 0%
	FW-02	Fail				
	FW-03	Fail				
	FW-04	Fail				
	FW-05	Pass				
	FW-06	Fail				
	FW-07	Fail				
	FW-08	Fail				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	2/10 20%	8/10 80%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Pass				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		25/66 38%	33/66 50%	0/66 0%	8/66 12%
			Pass	**Fail**	**Unknown**	**N/A**

StartVision

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Pass				
	HW-03	Fail				
	HW-04	Fail				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	0/5 0%	4/5 80%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Fail				
Mobile Security (MS)	MS-01	Pass	4/7 57%	1/7 14%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	0/8 0%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	4/6 67%	2/6 33%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		23/66 35%	13/66 20%	7/66 11%	23/66 35%
			Pass	**Fail**	**Unknown**	**N/A**

TP-Link

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	2/5 40%	3/5 60%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Pass				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	2/7 29%	0/7 0%	1/7 14%
	MS-02	Fail				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Pass				
Wi-Fi Security (WF)	WF-01	Pass	1/4 25%	3/4 75%	0/4 0%	0/4 0%
	WF-02	Fail				
	WF-03	Fail				
	WF-04	Fail				
Service Security (SS)	SS-01	Fail	6/11 55%	2/11 18%	0/11 0%	3/11 27%
	SS-02	Pass				
	SS-03	Pass				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	1/4 25%	0/4 0%	0/4 0%
	HW-02	Fail				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	6/8 75%	2/8 25%	0/8 0%	0/8 0%
	FW-02	Pass				
	FW-03	Pass				
	FW-04	Pass				
	FW-05	Fail				
	FW-06	Pass				
	FW-07	Fail				
	FW-08	Pass				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	EP-02	Pass				
	EP-03	Fail				
	EP-04	Fail				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	Pass	3/6 50%	3/6 50%	0/6 0%	0/6 0%
	BH-02	Fail				
	BH-03	Pass				
	BH-04	Fail				
	BH-05	Pass				
	BH-06	Fail				
Linux Hardening (LH)	LH-01	Fail	1/10 10%	9/10 90%	0/10 0%	0/10 0%
	LH-02	Fail				
	LH-03	Fail				
	LH-04	Fail				
	LH-05	Fail				
	LH-06	Fail				
	LH-07	Fail				
	LH-08	Fail				
	LH-09	Fail				
	LH-10	Pass				
	Grand Total		30/66 45%	31/66 47%	0/66 0%	5/66 8%
			Pass	**Fail**	**Unknown**	**N/A**

Vacos

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Fail	3/7 43%	4/7 57%	0/7 0%	0/7 0%
	MS-02	Fail				
	MS-03	Fail				
	MS-04	Pass				
	MS-05	Pass				
	MS-06	Pass				
	MS-07	Fail				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	5/11 45%	1/11 9%	0/11 0%	5/11 45%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	N/A				
	HW-01	Pass	3/4 75%	0/4 0%	1/4 25%	0/4 0%
	HW-02	Unknown				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	4/8 50%	2/8 25%	2/8 25%	0/8 0%
	FW-02	Fail				
	FW-03	Fail				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Pass				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	2/6 33%	2/6 33%	0/6 0%	2/6 33%
	EP-02	Fail				
	EP-03	N/A				
	EP-04	N/A				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		21/66 32%	17/66 26%	3/66 5%	25/66 38%
			Pass	**Fail**	**Unknown**	**N/A**

WOHOME

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Integrity (HW)	HW-01	Fail	1/5 20%	4/5 80%	0/5 0%	0/5 0%
	HW-02	Fail				
	HW-03	Fail				
	HW-04	Pass				
	HW-05	Fail				
Local Access (LA)	LA-01	Fail	1/5 20%	3/5 60%	0/5 0%	1/5 20%
	LA-02	Fail				
	LA-03	N/A				
	LA-04	Fail				
	LA-05	Pass				
Mobile Security (MS)	MS-01	Pass	4/7 57%	1/7 14%	1/7 14%	1/7 14%
	MS-02	Pass				
	MS-03	Pass				
	MS-04	Pass				
	MS-05	Fail				
	MS-06	N/A				
	MS-07	Unknown				
Wi-Fi Security (WF)	WF-01	Pass	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	WF-02	Fail				
	WF-03	Pass				
	WF-04	N/A				
Service Security (SS)	SS-01	Pass	6/11 55%	1/11 9%	0/11 0%	4/11 36%
	SS-02	N/A				
	SS-03	N/A				
	SS-04	Pass				
	SS-05	Pass				
	SS-06	Pass				
	SS-07	N/A				
	SS-08	N/A				
	SS-09	Fail				
	SS-10	Pass				
	SS-11	Pass				
	HW-01	Fail	2/4 50%	1/4 25%	0/4 0%	1/4 25%
	HW-02	N/A				

Category	ID	Status	Pass	Fail	Unknown	N/A
Hardware Security (HW)	HW-03	Pass				
	HW-04	Pass				
Firmware Updates (FW)	FW-01	Pass	3/8 38%	0/8 0%	5/8 63%	0/8 0%
	FW-02	Unknown				
	FW-03	Unknown				
	FW-04	Pass				
	FW-05	Unknown				
	FW-06	Pass				
	FW-07	Unknown				
	FW-08	Unknown				
End-user Privacy (EP)	EP-01	Pass	3/6 50%	2/6 33%	1/6 17%	0/6 0%
	EP-02	Unknown				
	EP-03	Fail				
	EP-04	Pass				
	EP-05	Pass				
	EP-06	Fail				
Binary Hardening (BH)	BH-01	N/A	0/6 0%	0/6 0%	0/6 0%	6/6 100%
	BH-02	N/A				
	BH-03	N/A				
	BH-04	N/A				
	BH-05	N/A				
	BH-06	N/A				
Linux Hardening (LH)	LH-01	N/A	0/10 0%	0/10 0%	0/10 0%	10/10 100%
	LH-02	N/A				
	LH-03	N/A				
	LH-04	N/A				
	LH-05	N/A				
	LH-06	N/A				
	LH-07	N/A				
	LH-08	N/A				
	LH-09	N/A				
	LH-10	N/A				
	Grand Total		22/66 33%	13/66 20%	7/66 11%	24/66 36%
			Pass	**Fail**	**Unknown**	**N/A**

APPENDIX C: ETSI – TEST CRITERIA DATA MAPPING

Test Case	Combined Criteria to Pass the Test
5.1-1	- No Linux accounts with passwords are set
5.1-2	- No Linux accounts with passwords are set - No default device passwords are set - No hardcoded Wi-Fi pairing password is set
5.1-3	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server
5.1-4	- No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service without a custom password - No local HTTP service without a custom password
5.1-5	- No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - No local HTTP service is enabled by default
5.2-1	- A published vendor security policy was found
5.2-2	- Out of scope for this research
5.2-3	- Linux kernel is based on a supported code train - No Linux accounts with passwords are set - A firmware update mechanism is provided
5.3-1	- All firmware updates are sent over HTTPS - A firmware update mechanism is provided
5.3-2	- All firmware updates are sent over HTTPS - A firmware update mechanism is provided - Secure Boot is available and actively in use - Firmware is digitally signed by the vendor
5.3-3	- A firmware update mechanism is provided
5.3-4	- A firmware update mechanism is provided - The end-user is notified of a firmware update - The end-user can check for a firmware update
5.3-5	- A firmware update mechanism is provided - The end-user is notified of a firmware update
5.3-6	- Firmware updates are not forced upon an end-user - A firmware update mechanism is provided

Test Case	Combined Criteria to Pass the Test
5.3-7	- All firmware updates are sent over HTTPS - A firmware update mechanism is provided
5.3-8	- A firmware update mechanism is provided - The end-user is notified of a firmware update - The end-user can check for a firmware update
5.3-9	- Firmware with a digital signature is verified before use - Firmware with a cryptographic hash is verified before use - Secure Boot is available and actively in use - A firmware update mechanism is provided
5.3-10	- Firmware with a digital signature is verified before use - All firmware updates are sent over HTTPS - A firmware update mechanism is provided
5.3-11	- A firmware update mechanism is provided - The end-user is notified of a firmware update
5.3-12	- Out of scope for this research
5.3-13	- Out of scope for this research
5.3-14	- Out of scope for this research
5.3-15	- Out of scope for this research
5.3-16	- The device features a model designation by the vendor
5.4-1	- Secure Boot is available and actively in use - The device's filesystem is encrypted at rest
5.4-2	- Out of scope for this research
5.4-3	- No Linux accounts with passwords are set - No local RTSP service without a custom password - No local HTTP service without a custom password
5.4-4	- Out of scope for this research
5.5-1	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server - All firmware updates are sent over HTTPS
5.5-2	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server - All firmware updates are sent over HTTPS

Test Case	Combined Criteria to Pass the Test
5.5-3	- A firmware update mechanism is provided
5.5-4	- No local RTSP service without a custom password - No local HTTP service without a custom password
5.5-5	- Out of scope for this research
5.5-6	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server
5.5-7	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server
5.5-8	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server
5.6-1	- No local telnet service is enabled by default - No local FTP service is enabled by default
5.6-2	- Out of scope for this research
5.6-3	- Device USB ports do not allow for mounting device storage - Device USB ports do not allow a debug interface (e.g., *adb*)
5.6-4	- No unauthenticated bootloader access is available - No unauthenticated OS login shell is available - No OS login prompt is available
5.6-5	- No local telnet service is enabled by default - No local FTP service is enabled by default
5.6-6	- Out of scope for this research
5.6-7	- Most Linux processes do not run as the root user
5.6-8	- The device's CPU has a supported MMU
5.6-9	- Stack canaries are in use on system binaries - NX memory pages are in use on system binaries
5.7-1	- Secure Boot is available and actively in use
5.7-2	- Out of scope for this research
5.8-1	- All local web servers only support HTTPS - No local telnet service is enabled by default

Test Case	Combined Criteria to Pass the Test
	- No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server
5.8-2	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server
5.8-3	- Out of scope for this research
5.9-1	- Out of scope for this research
5.9-2	- Out of scope for this research
5.9-3	- Out of scope for this research
5.10-1	- Out of scope for this research
5.11-1	- The device has a physical factory-reset mechanism - All sensitive data is removed with a factory reset
5.11-2	- Out of scope for this research
5.11-3	- The device has a physical factory-reset mechanism - All sensitive data is removed with a factory reset
5.11-4	- The device has a physical factory-reset mechanism - All sensitive data is removed with a factory reset
5.12-1	- Out of scope for this research
5.12-2	- A user manual is provided by the vendor
5.12-3	- Out of scope for this research
5.13-1	- Out of scope for this research

APPENDIX D: ETSI – CAMERA MAPPING

Baby Monitors

CellBee

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1 5.1-2 5.1-3 5.1-4 5.1-5	Fail Fail Fail Fail Fail	0/5 0%	5/5 100%
Implement a means to manage reports of vulnerabilities	5.2-1 5.2-3	Fail Fail	0/2 0%	2/2 100%
Keep software updated	5.3-1 5.3-2 5.3-3 5.3-4 5.3-5 5.3-6 5.3-7 5.3-8 5.3-9 5.3-10 5.3-11 5.3-16	Pass Fail Pass Fail Fail Fail Pass Fail Pass Pass Fail Pass	6/12 50%	6/12 50%
Securely store sensitive security parameters	5.4-1 5.4-3	Fail Fail	0/2 0%	2/2 100%
Communicate securely	5.5-1 5.5-2 5.5-3 5.5-4 5.5-6 5.5-7 5.5-8	Fail Fail Pass Pass Fail Fail Fail	2/7 29%	5/7 71%
	5.6-1	Fail		

Category	ID	Status	Pass	Fail
Minimize exposed attack surfaces	5.6-3 5.6-4 5.6-5 5.6-7 5.6-8 5.6-9	Pass Fail Fail Fail Pass Fail	2/7 29%	5/7 71%
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		11/42 26%	31/42 74%
			Pass	**Fail**

Kami Baby

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	8/12 67%	4/12 33%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Fail		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Fail		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	5/7 71%	2/7 29%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

Category	ID	Status	Pass	Fail
	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		27/42 64%	15/42 36%
			Pass	**Fail**

Motorola

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	2/5 40%	3/5 60%
	5.1-2	Pass		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Pass	1/2 50%	1/2 50%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	6/12 50%	6/12 50%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		18/42 43%	24/42 57%
			Pass	**Fail**

Sense-U

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	1/12 8%	11/12 92%
	5.3-2	Fail		
	5.3-3	Fail		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Fail		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	6/7 86%	1/7 14%
	5.5-2	Pass		
	5.5-3	Fail		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		18/42 43%	24/42 57%
			Pass	**Fail**

VTech

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	8/12 67%	4/12 33%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Pass		
	5.3-6	Fail		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		25/42 60%	17/42 40%
			Pass	**Fail**

Doorbells

Energizer

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	11/12 92%	1/12 8%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		

Minimize exposed attack surfaces	5.6-1 5.6-3 5.6-4 5.6-5 5.6-7 5.6-8 5.6-9	Pass Pass Fail Pass Fail Pass Fail	4/7 57%	3/7 43%
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		21/42 50%	21/42 50%
			Pass	**Fail**

Euarne

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	10/12 83%	2/12 17%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		34/42 81% **Pass**	8/42 19% **Fail**

Eufy

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Pass	2/2 100%	0/2 0%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	6/12 50%	6/12 50%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		34/42 81%	8/42 19%
			Pass	**Fail**

Victure

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	3/5 60%	2/5 40%
	5.1-2	Pass		
	5.1-3	Fail		
	5.1-4	Pass		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	10/12 83%	2/12 17%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	7/7 100%	0/7 0%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		26/42 62%	16/42 38%
			Pass	**Fail**

Wuuk

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		33/42 79%	9/42 21%
			Pass	**Fail**

Hidden Cameras

Camakt

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	11/12 92%	1/12 8%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	7/7 100%	0/7 0%
	5.6-3	Pass		
	5.6-4	Pass		

	5.6-5 5.6-7 5.6-8 5.6-9	Pass Pass Pass Pass		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		37/42 88% **Pass**	5/42 12% **Fail**

Ecwey

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	10/12 83%	2/12 17%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Fail	2/7 29%	5/7 71%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Fail		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		18/42 43%	24/42 57%
			Pass	**Fail**

Pambrum

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	1/12 8%	11/12 92%
	5.3-2	Fail		
	5.3-3	Fail		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Fail		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Fail		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Fail	2/7 29%	5/7 71%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Fail		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		8/42 19%	34/42 81%
			Pass	**Fail**

Swept Supplies

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	1/5 20%	4/5 80%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	1/12 8%	11/12 92%
	5.3-2	Fail		
	5.3-3	Fail		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Fail		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Fail		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Fail	3/7 43%	4/7 57%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Fail		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		12/42 29%	30/42 71%
			Pass	**Fail**

VicZone

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	1/12 8%	11/12 92%
	5.3-2	Fail		
	5.3-3	Fail		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Fail		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	0/7 0%	7/7 100%
	5.5-2	Fail		
	5.5-3	Fail		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Fail	2/7 29%	5/7 71%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Fail		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		8/42 19%	34/42 81%
			Pass	**Fail**

Pet Feeders

Didog

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1 5.1-2 5.1-3 5.1-4 5.1-5	Fail Fail Fail Fail Fail	0/5 0%	5/5 100%
Implement a means to manage reports of vulnerabilities	5.2-1 5.2-3	Fail Fail	0/2 0%	2/2 100%
Keep software updated	5.3-1 5.3-2 5.3-3 5.3-4 5.3-5 5.3-6 5.3-7 5.3-8 5.3-9 5.3-10 5.3-11 5.3-16	Fail Fail Pass Fail Fail Fail Fail Fail Pass Fail Fail Pass	3/12 25%	9/12 75%
Securely store sensitive security parameters	5.4-1 5.4-3	Fail Fail	0/2 0%	2/2 100%
Communicate securely	5.5-1 5.5-2 5.5-3 5.5-4 5.5-6 5.5-7 5.5-8	Fail Fail Pass Pass Fail Fail Fail	2/7 29%	5/7 71%
Minimize exposed attack surfaces	5.6-1 5.6-3 5.6-4	Fail Pass Fail	2/7 29%	5/7 71%

	5.6-5 5.6-7 5.6-8 5.6-9	Fail Fail Pass Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		12/42 29%	30/42 71%
			Pass	**Fail**

HONGSA

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	4/12 33%	8/12 67%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Pass		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Fail	2/7 29%	5/7 71%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Fail		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		9/42 21%	33/42 79%
			Pass	**Fail**

IOIODOG

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		33/42 79%	9/42 21%
			Pass	**Fail**

iSmartPet

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1 5.1-2 5.1-3 5.1-4 5.1-5	Fail Fail Fail Fail Fail	0/5 0%	5/5 100%
Implement a means to manage reports of vulnerabilities	5.2-1 5.2-3	Fail Fail	0/2 0%	2/2 100%
Keep software updated	5.3-1 5.3-2 5.3-3 5.3-4 5.3-5 5.3-6 5.3-7 5.3-8 5.3-9 5.3-10 5.3-11 5.3-16	Fail Fail Fail Fail Fail Fail Fail Fail Fail Fail Fail Pass	1/12 8%	11/12 92%
Securely store sensitive security parameters	5.4-1 5.4-3	Fail Fail	0/2 0%	2/2 100%
Communicate securely	5.5-1 5.5-2 5.5-3 5.5-4 5.5-6 5.5-7 5.5-8	Fail Fail Fail Fail Fail Fail Fail	0/7 0%	7/7 100%
Minimize exposed attack surfaces	5.6-1 5.6-3 5.6-4 5.6-5 5.6-7 5.6-8	Fail Pass Fail Fail Fail Pass	2/7 29%	5/7 71%

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		8/42 19%	34/42 81%
			Pass	**Fail**

Sekoya

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Fail	2/7 29%	5/7 71%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Fail		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		17/42 40%	25/42 60%
			Pass	**Fail**

Security Cameras

Akaso

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1 5.1-2 5.1-3 5.1-4 5.1-5	Pass Pass Fail Fail Fail	2/5 40%	3/5 60%
Implement a means to manage reports of vulnerabilities	5.2-1 5.2-3	Fail Pass	1/2 50%	1/2 50%
Keep software updated	5.3-1 5.3-2 5.3-3 5.3-4 5.3-5 5.3-6 5.3-7 5.3-8 5.3-9 5.3-10 5.3-11 5.3-16	Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass	12/12 100%	0/12 0%
Securely store sensitive security parameters	5.4-1 5.4-3	Pass Fail	1/2 50%	1/2 50%
Communicate securely	5.5-1 5.5-2 5.5-3 5.5-4 5.5-6 5.5-7 5.5-8	Fail Fail Pass Fail Fail Fail Fail	1/7 14%	6/7 86%
Minimize exposed attack surfaces	5.6-1 5.6-3 5.6-4	Pass Pass Pass	7/7 100%	0/7 0%

	5.6-5 5.6-7 5.6-8 5.6-9	Pass Pass Pass Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		29/42 69% **Pass**	13/42 31% **Fail**

Amcrest

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	3/5 60%	2/5 40%
	5.1-2	Pass		
	5.1-3	Fail		
	5.1-4	Pass		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	7/7 100%	0/7 0%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		30/42 71%	12/42 29%
			Pass	**Fail**

Anbes

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	2/5 40%	3/5 60%
	5.1-2	Pass		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	10/12 83%	2/12 17%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	7/7 100%	0/7 0%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		27/42 64%	15/42 36%
			Pass	**Fail**

Anran

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	7/12 58%	5/12 42%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	5/7 71%	2/7 29%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		14/42 33%	28/42 67%
			Pass	**Fail**

Aqara

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	1/5 20%	4/5 80%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Pass		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	7/12 58%	5/12 42%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Fail		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		15/42 36%	27/42 64%
			Pass	**Fail**

Conico

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	2/5 40%	3/5 60%
	5.1-2	Pass		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Fail	8/12 67%	4/12 33%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Fail		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Fail		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	7/7 100%	0/7 0%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		25/42 60%	17/42 40%
			Pass	**Fail**

DCT

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	11/12 92%	1/12 8%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Fail		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		35/42 83%	7/42 17%
			Pass	**Fail**

Ecobee

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	3/5 60%	2/5 40%
	5.1-2	Pass		
	5.1-3	Fail		
	5.1-4	Pass		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Pass	2/2 100%	0/2 0%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	10/12 83%	2/12 17%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Fail		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	5/7 71%	2/7 29%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		28/42 67%	14/42 33%
			Pass	**Fail**

Eversecu

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	4/5 80%	1/5 20%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		38/42 90%	4/42 10%
			Pass	**Fail**

Feit Electric

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	11/12 92%	1/12 8%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	5/7 71%	2/7 29%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		32/42 76%	10/42 24%
			Pass	**Fail**

HeimVision

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	1/7 14%	6/7 86%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		22/42 52%	20/42 48%
			Pass	**Fail**

Jennov

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	0/5 0%	5/5 100%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Fail		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	1/12 8%	11/12 92%
	5.3-2	Fail		
	5.3-3	Fail		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Fail		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	0/7 0%	7/7 100%
	5.5-2	Fail		
	5.5-3	Fail		
	5.5-4	Fail		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	5/7 71%	2/7 29%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		7/42 17%	35/42 83%
			Pass	**Fail**

LaView

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	5/7 71%	2/7 29%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		31/42 74%	11/42 26%
			Pass	**Fail**

Mascarry

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	9/12 75%	3/12 25%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Fail		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	5/7 71%	2/7 29%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	5/7 71%	2/7 29%
	5.6-3	Pass		
	5.6-4	Pass		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		29/42 69%	13/42 31%
			Pass	**Fail**

Moonxiao

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	1/5 20%	4/5 80%
	5.1-2	Fail		
	5.1-3	Fail		
	5.1-4	Pass		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	4/12 33%	8/12 67%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Pass		
	5.3-7	Fail		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Fail		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	2/7 29%	5/7 71%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Fail		
	5.5-7	Fail		
	5.5-8	Fail		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Fail Fail	0/2 0%	2/2 100%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		16/42 38%	26/42 62%
			Pass	**Fail**

Reolink

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	3/5 60%	2/5 40%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	0/2 0%	2/2 100%
	5.2-3	Fail		
Keep software updated	5.3-1	Pass	6/12 50%	6/12 50%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Fail		
	5.3-10	Pass		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		26/42 62%	16/42 38%
			Pass	**Fail**

StartVision

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		39/42 93%	3/42 7%
			Pass	**Fail**

TP-Link

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Fail	2/5 40%	3/5 60%
	5.1-2	Fail		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Fail		
Implement a means to manage reports of vulnerabilities	5.2-1	Pass	1/2 50%	1/2 50%
	5.2-3	Fail		
Keep software updated	5.3-1	Fail	8/12 67%	4/12 33%
	5.3-2	Fail		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Fail		
	5.3-7	Fail		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	0/2 0%	2/2 100%
	5.4-3	Fail		
Communicate securely	5.5-1	Fail	5/7 71%	2/7 29%
	5.5-2	Fail		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	4/7 57%	3/7 43%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Fail		
	5.6-8	Pass		

	5.6-9	Fail		
Ensure software integrity	5.7-1	Fail	0/1 0%	1/1 100%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		26/42 62%	16/42 38%
			Pass	**Fail**

Vacos

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	8/12 67%	4/12 33%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Fail		
	5.3-5	Fail		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Fail		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Fail		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Fail Fail Fail	0/3 0%	3/3 100%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		32/42 76%	10/42 24%
			Pass	**Fail**

WOHOME

Category	ID	Status	Pass	Fail
No universal default passwords	5.1-1	Pass	5/5 100%	0/5 0%
	5.1-2	Pass		
	5.1-3	Pass		
	5.1-4	Pass		
	5.1-5	Pass		
Implement a means to manage reports of vulnerabilities	5.2-1	Fail	1/2 50%	1/2 50%
	5.2-3	Pass		
Keep software updated	5.3-1	Pass	12/12 100%	0/12 0%
	5.3-2	Pass		
	5.3-3	Pass		
	5.3-4	Pass		
	5.3-5	Pass		
	5.3-6	Pass		
	5.3-7	Pass		
	5.3-8	Pass		
	5.3-9	Pass		
	5.3-10	Pass		
	5.3-11	Pass		
	5.3-16	Pass		
Securely store sensitive security parameters	5.4-1	Fail	1/2 50%	1/2 50%
	5.4-3	Pass		
Communicate securely	5.5-1	Pass	7/7 100%	0/7 0%
	5.5-2	Pass		
	5.5-3	Pass		
	5.5-4	Pass		
	5.5-6	Pass		
	5.5-7	Pass		
	5.5-8	Pass		
Minimize exposed attack surfaces	5.6-1	Pass	6/7 86%	1/7 14%
	5.6-3	Pass		
	5.6-4	Fail		
	5.6-5	Pass		
	5.6-7	Pass		
	5.6-8	Pass		

	5.6-9	Pass		
Ensure software integrity	5.7-1	Pass	1/1 100%	0/1 0%
Ensure that personal data is secure	5.8-1 5.8-2	Pass Pass	2/2 100%	0/2 0%
Make it easy for users to delete user data	5.11-1 5.11-3 5.11-4	Pass Pass Pass	3/3 100%	0/3 0%
Make installation and maintenance of devices easy	5.12-2	Pass	1/1 100%	0/1 0%
	Grand Total		39/42 93%	3/42 7%
			Pass	**Fail**

APPENDIX E: DCMS – TEST CRITERIA DATA MAPPING

ID	Title	Combined Criteria to Pass the Test
1	No default passwords	- No Linux accounts with passwords are set - No default device passwords are set - No hardcoded Wi-Fi pairing password is set
2	Implement a vulnerability disclosure policy	- A published vendor security policy was found
3	Keep software updated	- A firmware update mechanism is provided - The end-user is notified of a firmware update - The end-user can check for a firmware update
4	Securely store credentials and security-sensitive data	- No Linux accounts with passwords are set
5	Communicate securely	- All local web servers only support HTTPS - No local telnet service is enabled by default - No local FTP service is enabled by default - No local RTSP service is enabled by default - All MQTT usage is encrypted with the server - All firmware updates are sent over HTTPS
6	Minimise exposed attack surfaces	- No unauthenticated bootloader access is available - No unauthenticated OS login shell is available - No local telnet service is enabled by default - No local FTP service is enabled by default - No local SSH service is enabled by default
7	Ensure software integrity	- All firmware updates are sent over HTTPS - Secure Boot is available and actively in use - Firmware is digitally signed by the vendor
8	Ensure that personal data is protected	- Out of scope for this research
9	Make systems resilient to outages	- Out of scope for this research
10	Monitor system telemetry data	- Out of scope for this research
11	Make it easy for consumers to delete personal data	- All sensitive data is removed with a factory reset
12	Make installation and maintenance of devices easy	- A user manual is provided by the vendor
13	Validate input data	- Out of scope for this research

APPENDIX F: DCMS - CAMERA MAPPING

Vendor	ID 01	ID 02	ID 03	ID 04	ID 05	ID 06	ID 07	ID 11	ID 12	Pass	Fail
Akaso	Pass	Fail	Pass	Pass	Fail	Pass	Pass	Pass	Pass	7/9 78%	2/9 22%
Amcrest	Pass	Fail	Pass	Pass	Fail	Pass	Pass	Pass	Pass	7/9 78%	2/9 22%
Anbes	Pass	Fail	Fail	Pass	Fail	Pass	Pass	Pass	Pass	6/9 67%	3/9 33%
Anran	Fail	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Pass	2/9 22%	7/9 78%
Aqara	Fail	Fail	Pass	Fail	Fail	Pass	Fail	Fail	Pass	3/9 33%	6/9 67%
Camakt	Pass	Fail	Pass	Pass	Pass	Pass	Fail	Pass	Pass	7/9 78%	2/9 22%
CellBee	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Pass	1/9 11%	8/9 89%
Conico	Pass	Fail	Pass	Pass	Fail	Pass	Fail	Pass	Pass	6/9 67%	3/9 33%
DCT	Pass	Fail	Pass	Pass	Pass	Pass	Pass	Fail	Pass	7/9 78%	2/9 22%
Didog	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	2/9 22%	7/9 78%
Ecobee	Pass	Pass	Pass	Pass	Fail	Pass	Fail	Pass	Pass	7/9 78%	2/9 22%
Ecwey	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	Pass	3/9 33%	6/9 67%
Energizer	Fail	Fail	Pass	Fail	Fail	Pass	Fail	Pass	Pass	4/9 44%	5/9 56%
Euarne	Pass	Fail	Fail	Pass	Pass	Fail	Pass	Fail	Pass	5/9 56%	4/9 44%
Eufy	Pass	Pass	Fail	Pass	Pass	Pass	Fail	Pass	Pass	7/9 78%	2/9 22%
Eversecu	Fail	Fail	Pass	Pass	Pass	Fail	Pass	Pass	Pass	6/9 67%	3/9 33%

Vendor	ID 01	ID 02	ID 03	ID 04	ID 05	ID 06	ID 07	ID 11	ID 12	Pass	Fail
Feit Electric	Fail	Fail	Pass	Fail	Pass	Pass	Fail	Pass	Pass	5/9 56%	4/9 44%
HeimVision	Fail	Fail	Pass	Fail	Fail	Fail	Pass	Pass	Pass	4/9 44%	5/9 56%
HONGSA	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Pass	1/9 11%	8/9 89%
IOIODOG	Fail	Fail	Pass	Fail	Pass	Fail	Pass	Pass	Pass	5/9 56%	4/9 44%
iSmartPet	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	Pass	3/9 33%	6/9 67%
Jennov	Fail	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Pass	2/9 22%	7/9 78%
Kami Baby	Fail	Fail	Pass	Fail	Fail	Fail	Fail	Pass	Pass	3/9 33%	6/9 67%
LaView	Fail	Fail	Pass	Fail	Pass	Pass	Pass	Fail	Pass	5/9 56%	4/9 44%
Mascarry	Fail	Fail	Pass	Fail	Fail	Pass	Fail	Pass	Pass	4/9 44%	5/9 56%
Moonxiao	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	2/9 22%	7/9 78%
Motorola	Pass	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Pass	6/9 67%	3/9 33%
Pambrum	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	2/9 22%	7/9 78%
Reolink	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Pass	Pass	3/9 33%	6/9 67%
Sekoya	Fail	Fail	Pass	Fail	Fail	Fail	Pass	Fail	Pass	3/9 33%	6/9 67%
Sense-U	Fail	Fail	Fail	Fail	Pass	Pass	Pass	Fail	Pass	4/9 44%	5/9 56%
Start Vision	Pass	Fail	Pass	Pass	Pass	Fail	Pass	Pass	Pass	7/9 78%	2/9 22%
Swept Supplies	Fail	Fail	Fail	Pass	Fail	Fail	Pass	Pass	Pass	4/9 44%	5/9 56%

Vendor	ID 01	ID 02	ID 03	ID 04	ID 05	ID 06	ID 07	ID 11	ID 12	Pass	Fail
TP-Link	Fail	Pass	Pass	Fail	Fail	Fail	Fail	Pass	Pass	4/9 44%	5/9 56%
Vacos	Pass	Fail	Fail	Pass	Pass	Fail	Pass	Fail	Pass	5/9 56%	4/9 44%
Victure	Pass	Fail	Fail	Pass	Fail	Pass	Pass	Fail	Pass	5/9 56%	4/9 44%
VicZone	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	Pass	3/9 33%	6/9 67%
VTech	Fail	Fail	Fail	Fail	Pass	Fail	Fail	Fail	Pass	2/9 22%	7/9 78%
WOHOME	Pass	Fail	Pass	Pass	Pass	Fail	Pass	Pass	Pass	7/9 78%	2/9 22%
Wuuk	Fail	Fail	Pass	Fail	Pass	Pass	Pass	Pass	Pass	6/9 67%	3/9 33%

APPENDIX G: SAMPLE DEVICE FINDINGS

Baby Monitors

CellBee

Device Overview

Model: SC-AI04	**Released:** Aug, 2020	**Price:** $102.73

FCC ID: 2AS4ASCAI01	**Amazon:** B08FMK21MC	**UPC:** 850012821410

Product: https://www.simcam.ai/simcam-baby

Manual: https://fccid.io/2AS4ASC-AI04/User-Manual/User-Manual-4928135.pdf

Device ID: 5f2f95b20f80612914991a00	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Ingenic T31	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q128JVSQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: Yes	**Internal:** No

External Interfaces

USB Usage

Type: USB C	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 30:4A:26:2A:36:8A	**2.4GHz:** Yes	**5GHz:** Yes

Chipset: RTL8811CU	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: Yes	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** SPL 2013.07	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** Yes

User Can Request Update: No	**User Can Manually Install:** Yes

Firmware Security

Update Encrypted: No	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: Yes	**SSL Labs Score:** B	**Authentication:** No

Companion Mobile Application

Application Overview

Name: SimHome	**ID:** com.simshine.aiot

Tested Version: 1.2.4	**Released:** 08/12/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** None

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.10.14	**Date:** 05/20/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** Yes	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: babymonitor	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** sha512

Kami Baby

Device Overview

Model: Kami Baby Monitor	**Released:** Nov, 2020	**Price:** $99.99

FCC ID: 2AFIB-YYS5019	**Amazon:** B07PYTWTML	**UPC:** 6970171175750

Product: https://kamihome.com/kamibaby/

Manual: https://fccid.io/2AFIB-YYS5019/User-Manual/user-manual-4820166.pdf

Device ID: TNPUSAK-898731-PDPMX	**Serial:** BY501CUSO09002498

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: QG2101C	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH256BXIQ	**Type:** NAND

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** B8:C6:AA:1B:45:B0	**2.4GHz:** Yes	**5GHz:** No

Chipset: Unknown	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2018.05-00004-gf5d8011-dirty	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: XiaoYi Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Yes	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Kami Home	**ID:** com.yitechnology.kamihome

Tested Version: 2.7.4_20210711	**Released:** 07/12/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-16 characters (3 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.9.118	**Date:** Unknown	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** Yes

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: cloud	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** None

Motorola

Device Overview

Model: Connect40	**Released:** Jan, 2020	**Price:** $129.99

FCC ID: VLJ-CF85BU	**Amazon:** B081D7YKVQ	**UPC:** 816479018268

Product: https://motorolababy.com/product/connect40/

Manual: https://fccid.io/VLJ-CF85BU/User-Manual/User-Manual-5005208.pdf

Device ID: 016335000AE299CFB5LBXGSEQW	**Serial:** 434510H003877

Vendor Security Assertions

Security Policy: https://www.lenovo.com/us/en/product-security/reporting-a-vulnerability/

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: AK3918EN080	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: XT26G01BWSEG	**Type:** NAND

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** N/A	**Sensitive Data Cleared:** N/A

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: No	**Media Obfuscated:** N/A	**Format:** N/A

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 00:0A:E2:99:CF:B5	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8189FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: Unknown	**Version:** Unknown	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Anyka Linux	**Version:** 1.1.12	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** No	**Filesystem:** YAFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** Yes

User Can Request Update: Yes	**User Can Manually Install:** Yes

Firmware Security

Update Encrypted: Yes	**Hash Verification:** Yes	**Signed Image:** Yes

Transit Encryption: Yes	**SSL Labs Score:** B	**Authentication:** Yes

Companion Mobile Application

Application Overview

Name: Hubble Connected	**ID:** com.hubble.care

Tested Version: 1.01.21	**Released:** 08/21/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-30 characters (3 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 8080	**Encryption:** No	**Authentication:** No	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 08/07/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: crypto	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Present	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Unknown	**Hashing Algorithm:** Unknown

Sense-U

Device Overview

Model: SU-WA002	**Released:** Mar, 2020	**Price:** $129.99

FCC ID: Not Found	**Amazon:** B07YFCFCPN	**UPC:** None

Product: https://www.products.sense-u.com/sense-u-video-baby-monitor

Manual: https://shop.sense-u.com/pages/user-manual-video

Device ID: ebb599015f7907cabasgbx	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: RTS3903N	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** No	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q127CSIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 6A:57:2D:01:75:39	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 57600	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2014.01-v1.2	**Bootloader Access:** Password

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: No	**Notify User:** N/A	**Force Update:** N/A

User Can Request Update: N/A	**User Can Manually Install:** N/A

Firmware Security

Update Encrypted: N/A	**Hash Verification:** N/A	**Signed Image:** N/A

Transit Encryption: N/A	**SSL Labs Score:** N/A	**Authentication:** N/A

Companion Mobile Application

Application Overview

Name: Sense-U Baby Monitor New	**ID:** com.senseu.baby

Tested Version: 3.2.1	**Released:** 06/19/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 6+ characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 3.10.27	**Date:** 12/07/2018	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: tycam	**RELRO:** No	**Canary:** Yes	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** md5crypt

VTech

Device Overview

Model: VM901	**Released:** Mar, 2020	**Price:** $139.95

FCC ID: EW780-1957-00	**Amazon:** B07WCV632L	**UPC:** None

Product: https://www.vtechphones.com/amazon/vm901-smart-hd-video-baby-monitor

Manual: https://m.media-amazon.com/images/I/C1hn9d4VGgS.pdf

Device ID: BM1H59XJSSXYKRX5111A	**Serial:** 6C500098194

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: W25N01GVZEIG	**Type:** NAND

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** N/A	**Sensitive Data Cleared:** N/A

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: No	**Media Obfuscated:** N/A	**Format:** N/A

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 14:AE:DB:EB:94:23	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8189FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** YAFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** Yes

User Can Request Update: No	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Yes	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: Yes	**SSL Labs Score:** B	**Authentication:** No

Companion Mobile Application

Application Overview

Name: MyVTech Baby 1080p	**ID:** com.cams.vtech.mvb

Tested Version: 4.1.0.92	**Released:** 08/17/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** Yes	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-12 characters (2 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.9.37	**Date:** 10/11/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: vt_cam	**RELRO:** Partial	**Canary:** Yes	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Doorbells

Energizer

Device Overview

Model: EOD1-1002-SIL	**Released:** Mar, 2020	**Price:** $49.99

FCC ID: 2AG7C-BELL5S	**Amazon:** B085T8LNLP	**UPC:** 805106870409

Product: https://energizerconnect.com/product/smart-1080p-video-doorbell/

Manual: https://fccid.io/2AG7CBELL5S/User-Manual/User-Manual-4487207.pdf

Device ID: eb980fb023917c02aesqu6	**Serial:** 058172967

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** AC:5D:5C:F9:09:D1	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11-svn2	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** CramFS

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Energizer Connect	**ID:** com.xtreme.energizer

Tested Version: 4.2.0	**Released:** 04/20/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** Yes	***Required:*** No

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 4.9.37	**Date:** 07/22/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yew

Binary Hardening

Sample: ppsapp	**RELRO:** Partial	**Canary:** Yes	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** md5crypt

Euarne

Device Overview

Model: K-BELL 1c	**Released:** Jul, 2020	**Price:** $47.69

FCC ID: Not Found	**Amazon:** B08CWRDPSC	**UPC:** 610452767453

Product: Not Found

Manual: Not Found

Device ID: eb5017d44379fdc64crzdc	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v200	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64FWSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** D4:D2:D6:38:85:1E	**2.4GHz:** Yes	**5GHz:** No

Chipset: 3131A-S	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 1.4.6	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: No	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Smart Life	**ID:** com.tuya.smartlife

Tested Version: 3.29.5	**Released:** 07/31/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** Yes	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Eufy

Device Overview

Model: T8222	**Released:** Jul, 2020	**Price:** $129.99

FCC ID: 2AOKB-TB220	**Amazon:** B08DXD8LSR	**UPC:** None

Product: https://us.eufylife.com/products/e8222113

Manual: https://tinyurl.com/manual-eufy

Device ID: N/A	**Serial:** T8222P0020341D44

Vendor Security Assertions

Security Policy: https://us.eufylife.com/pages/vulnerability-disclosure-policy

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q128JVSQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** EXT4

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 8C:85:80:52:92:C8	**2.4GHz:** Yes	**5GHz:** No

Chipset: XR871	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: Yes	**Version:** 5	**Manual Pairing:** No	**PIN Required:** No

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** WLAN	**Other Baud Rate:** 115200

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 1.0.1.0	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** Yes

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: No	**Hash Verification:** No	**Signed Image:** No

Transit Encryption: Yes	**SSL Labs Score:** B	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Eufy Security	**ID:** com.oceanwing.battery.cam

Tested Version: 3.2.1_1030	**Released:** 08/11/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-20 characters (4 classes)

Two-Step Authentication:	***Available:*** Yes	***Required:*** No

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Victure

Device Overview

Model: VD300	**Released:** Feb, 2020	**Price:** $54.99

FCC ID: 2AREL-VD300	**Amazon:** B084DNJHDL	**UPC:** None

Product: https://govicture.com/products/victure-video-doorbell-wireless-wifi-only-2-4g

Manual: https://m.media-amazon.com/images/I/B1DxN8Dz+1S.pdf

Device ID: ppsl3086bd5f1dbd4e79	**Serial:** 060076586

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** AC:64:CF:FA:29:6E	**2.4GHz:** Yes	**5GHz:** No

Chipset: 3131A-S	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11-g52cd25b-dirty	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 1.0.0.5	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: No	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: CloudEdge	**ID:** com.cloudedge.smarteye

Tested Version: 3.0.5	**Released:** 07/16/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: No	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 1883	**Encryption:** No

Wuuk

Device Overview

Model: W0001	**Released:** Oct, 2020	**Price:** $89.00

FCC ID: 2AWHY-W0001	**Amazon:** B08K3L1SPY	**UPC:** 860003488805

Product: https://www.wuuklabs.com/

Manual: https://fccid.io/2AWHY-W0001/User-Manual/user-manual-4740419.pdf

Device ID: N/A	**Serial:** HXNAP1N81IWGL6BM

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: MT7628NN	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: W25Q128BV	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** B2:B3:53:06:ED:C6	**2.4GHz:** Yes	**5GHz:** No

Chipset: XR871	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 57600	**Other UART:** WLAN	**Other Baud Rate:** 115200

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2013.07	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** Yes	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Wuuk	**ID:** com.wuuklabs.android.store

Tested Version: 3.1.0	**Released:** 08/13/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8+ characters

Two-Step Authentication:	***Available:*** Yes	***Required:*** No

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 3.18.27	**Date:** 10/25/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: Ppcs_xmitech	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** Yes

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Hidden Cameras

Camakt

Device Overview

Model: WiFi Picture Photo Frame	**Released:** Dec, 2020	**Price:** $56.99

FCC ID: Not Found	**Amazon:** B08PK6NNPP	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: DV-44231152	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: AK3918EN080	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64FSIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 68:B9:D3:DD:1A:2E	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2013.10.0-AK_V2.0.04	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Anyka Linux	**Version:** 2.5.02	**Encrypted at Rest:** Unknown

Flash Dump Acquired: No	**Filesystem Scraped:** No	**Filesystem:** Unknown

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: DV380	**ID:** com.macrovideo.dv380

Tested Version: 1.0.21	**Released:** 07/20/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 6-16 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** Unknown	**IMA Used:** No

Signed Modules: Unknown	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: Unknown	**Mandatory (MAC) Used:** Unknown

Process Management

Most Root: Unknown	**cgroups:** Unknown	**seccomp:** Unknown	**Watchdog:** Unknown

Binary Hardening

Sample: Unknown	**RELRO:** Unknown	**Canary:** Unknown	**NX:** Unknown

Symbols: Unknown	**PIE:** Unknown	**Fortify:** Unknown	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Unknown	**Hashing Algorithm:** Unknown

Ecwey

Device Overview

Model: EV200	**Released:** Aug, 2020	**Price:** $51.29

FCC ID: Not Found	**Amazon:** B08GFF5WWZ	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: IVZ01-397743-MFSMT	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v200	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25L12835F	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: Yes	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** C0:99:58:B2:B8:71	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8201F	**WPA3 Support:** No	**WPS Support:** Yes

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: Yes	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: No	**User Can Manually Install:** Yes

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Ivzee	**ID:** com.rtp2p.Ivzee

Tested Version: 1.0.3	**Released:** 05/17/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** No	**Session Timeout:** No

Brute Force Protection: N/A	**Banner:** thttpd/2.25b 29dec2003

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 09/08/2017	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: vs_server	**RELRO:** No	**Canary:** Yes	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Pambrum

Device Overview

Model: spy cam clock-208	**Released:** Aug, 2020	**Price:** $55.99

FCC ID: Not Found	**Amazon:** B08GFQ5S8P	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: FHBB-142672-CYMNH	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64A-104HIP	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 2C:D2:6B:4F:1D:1C	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2013.10.0-AK_V3.0.08	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Anyka Linux	**Version:** 1.1.12	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: No	**Notify User:** N/A	**Force Update:** N/A

User Can Request Update: N/A	**User Can Manually Install:** N/A

Firmware Security

Update Encrypted: N/A	**Hash Verification:** N/A	**Signed Image:** N/A

Transit Encryption: N/A	**SSL Labs Score:** N/A	**Authentication:** N/A

Companion Mobile Application

Application Overview

Name: LookCam	**ID:** com.view.ppcs

Tested Version: V2021050801	**Released:** 05/13/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: N/A	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** Yes

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 11/12/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: anyka_ipc	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** Yes	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** md5crypt

Swept Supplies

Device Overview

Model: Ninja Pro Hidden Camera	**Released:** Aug, 2020	**Price:** $84.99

FCC ID: Not Found	**Amazon:** B08GBT5S51	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: TUT048299YZZXP	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Ingenic T21	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Mini B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 44:01:BB:1D:08:DD	**2.4GHz:** Yes	**5GHz:** No

Chipset: MT7601UN	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2013.07	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: No	**Notify User:** N/A	**Force Update:** N/A

User Can Request Update: N/A	**User Can Manually Install:** N/A

Firmware Security

Update Encrypted: N/A	**Hash Verification:** N/A	**Signed Image:** N/A

Transit Encryption: N/A	**SSL Labs Score:** N/A	**Authentication:** N/A

Companion Mobile Application

Application Overview

Name: LookCamPro	**ID:** com.shix.lookcam

Tested Version: 3.8	**Released:** 01/19/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: N/A	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.10.14	**Date:** 09/22/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** Yes	**seccomp:** No	**Watchdog:** No

Binary Hardening

Sample: target	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Unknown	**Hashing Algorithm:** Unknown

VicZone

Device Overview

Model: Y13	**Released:** Nov, 2020	**Price:** $94.99

FCC ID: Not Found	**Amazon:** B08NH7WN4W	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: WIN888-299148-KJURV	**Serial:** VVVIPC2004072413

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v200	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: DC Barrel	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 50:13:95:02:62:26	**2.4GHz:** Yes	**5GHz:** No

Chipset: MT7601UN	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Partial	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: No	**Notify User:** N/A	**Force Update:** N/A

User Can Request Update: N/A	**User Can Manually Install:** N/A

Firmware Security

Update Encrypted: N/A	**Hash Verification:** N/A	**Signed Image:** N/A

Transit Encryption: N/A	**SSL Labs Score:** N/A	**Authentication:** N/A

Companion Mobile Application

Application Overview

Name: WinCam Pro	**ID:** com.rtp2p.wincam

Tested Version: 1.1.5	**Released:** 04/10/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: N/A	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** 4 Hours

Brute Force Protection: No	**Banner:** thttpd/2.25b 29dec2003

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** No	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 09/09/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: vs_server	**RELRO:** No	**Canary:** Yes	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Pet Feeders

Didog

Device Overview

Model: FDB073-T980USA	**Released:** Jul, 2020	**Price:** $111.99

FCC ID: Not Found	**Amazon:** B08DKMQ3FD	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: PX2E6EU8ML9R9C52111A	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** N/A	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v200	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** N/A	**Sensitive Data Cleared:** N/A

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: USB A	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: No	**Media Obfuscated:** N/A	**Format:** N/A

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 20:32:33:A8:CA:62	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188ETV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** CPU	**Other Baud Rate:** 115200

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06-dirty	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** Yes

User Can Request Update: No	**User Can Manually Install:** Yes

Firmware Security

Update Encrypted: No	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: PetuNew	**ID:** cn.P2PPetCam.www.linyuan

Tested Version: 2.1.96	**Released:** 08/18/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 6-12 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 03/21/2018	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: IPServer	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

HONGSA

Device Overview

Model: Automatic Pet Feeder	**Released:** Aug, 2020	**Price:** $99.99

FCC ID: Not Found	**Amazon:** B08FR1S1GV	**UPC:** None

Product: http://www.chinaomg.com/product/3.html

Manual: Not Found

Device ID: HD99RC4FRXV65LP5111A	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: AK3918EN080	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 32:4A:26:76:AC:E7	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8189FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: spiboot	**Version:** 1.1.01	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: No	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Smart Pets	**ID:** com.aomeijia.cam

Tested Version: 1.0.8	**Released:** 10/14/2020	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** Yes

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 12/05/2018	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: daemon	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** md5crypt

IOIODOG

Device Overview

Model: Pet Auto Feeder	**Released:** Nov, 2020	**Price:** $123.49

FCC ID: Not Found	**Amazon:** B08P459F7R	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: eb8c28b3ce0fb124bacwfk	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: RTS3903N	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** No	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: DC Barrel	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 5E:56:4E:F9:01:E8	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 57600	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2014.01-v1.2	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Smart Life	**ID:** com.tuya.smartlife

Tested Version: 3.29.5	**Released:** 07/31/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** Yes	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.10.27	**Date:** 04/27/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: dgiot	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

iSmartPet

Device Overview

Model: 97089	**Released:** May, 2020	**Price:** $119.95

FCC ID: Not Found	**Amazon:** B087YWJ2ZZ	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: spf0909097410tatv	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v200	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q128JVSQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** N/A	**Sensitive Data Cleared:** N/A

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: No	**Media Obfuscated:** N/A	**Format:** N/A

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 34:20:03:28:90:47	**2.4GHz:** Yes	**5GHz:** Yes

Chipset: RTL8811CU	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** Yes	**Filesystem:** JFFS2

Firmware Updates

Update Support: No	**Notify User:** N/A	**Force Update:** N/A

User Can Request Update: N/A	**User Can Manually Install:** N/A

Firmware Security

Update Encrypted: N/A	**Hash Verification:** N/A	**Signed Image:** N/A

Transit Encryption: N/A	**SSL Labs Score:** N/A	**Authentication:** N/A

Companion Mobile Application

Application Overview

Name: iSmartPet	**ID:** com.ismartpet.pet

Tested Version: 2.01.10	**Released:** 01/10/2020	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** None

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** No	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 03/28/2018	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** Yes	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: v200smartlink	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** sha512

Sekoya

Device Overview

Model: PP003	**Released:** Nov, 2020	**Price:** $129.99

FCC ID: 2AXFT-PP003	**Amazon:** B08P1G2P8P	**UPC:** None

Product: Not Found

Manual: https://fccid.io/2AXFT-PP003/User-Manual/User-manual-5036803.pdf

Device ID: eb4a199b0606970b61adtb	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: GK7102C	**Processor:** ARM1176ZJFS	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Mini B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 0C:CF:89:EC:57:03	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2012.10	**Bootloader Access:** Password

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Pet Zero	**ID:** com.kkpetfeeder.petzero.android

Tested Version: 1.0.1	**Released:** 06/23/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters (2 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: Yes	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** No	**LED:** No

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 3.4.43	**Date:** 03/30/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** Yes	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: guard	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** Unknown

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** None

Security Cameras

Akaso

Device Overview

Model: CS300	**Released:** Jul, 2020	**Price:** $48.99

FCC ID: Not Found	**Amazon:** B08CRJMNYQ	**UPC:** None

Product: Not Found

Manual: https://www.akasotech.com/usermanual/cs300v2.pdf

Device ID: pp014896521fd0c7b205	**Serial:** 60609801

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** FC:6B:F0:A4:29:57	**2.4GHz:** Yes	**5GHz:** No

Chipset: Hi1131	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11-g3e11b05-dirty	**Bootloader Access:** Password

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 3.2.1	**Encrypted at Rest:** Yes

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Smart Life	**ID:** com.tuya.smartlife

Tested Version: 3.29.5	**Released:** 07/31/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** Yes	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 8090	**Encryption:** No	**Authentication:** No	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Amcrest

Device Overview

Model: ASH42	**Released:** Jan, 2020	**Price:** $50.99

FCC ID: ZZ2-Z10	**Amazon:** B083TLW9JL	**UPC:** 850007530969

Product: https://amcrest.com/amcrest-smarthome-ash42-w-white.html

Manual: https://fccid.io/ZZ2-Z10/User-Manual/User-Manual-4585698.pdf

Device ID: N/A	**Serial:** Z1080056AC450

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: DH6011	**Processor:** ARM	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Unknown	**Hardware PRNG:** Unknown

Secure Boot Available: Unknown	**TPM Available:** Yes

Flash Memory

Chipset: F50L1G41A	**Type:** NAND

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 9C:8E:CD:2F:FF:37	**2.4GHz:** Yes	**5GHz:** Yes

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: Yes	**MAC:** 9C:8E:CD:2F:F9:5F

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06-svn6637	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Yes

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Amcrest Smart Home	**ID:** com.mm.android.amcrestsmarthome

Tested Version: 3.9.1	**Released:** 06/02/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** Yes	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-32 characters (2 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** Yes	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.18.30	**Date:** Unknown	**IMA Used:** Unknown

Signed Modules: Unknown	**KASLR Used:** Unknown	**Secure Boot Used:** Unknown

Filesystem Access Controls

Discretionary Appropriate: Unknown	**Mandatory (MAC) Used:** Unknown

Process Management

Most Root: Unknown	**cgroups:** Unknown	**seccomp:** Unknown	**Watchdog:** Unknown

Binary Hardening

Sample: Unknown	**RELRO:** Unknown	**Canary:** Unknown	**NX:** Unknown

Symbols: Unknown	**PIE:** Unknown	**Fortify:** Unknown	**ASLR:** Unknown

Network Security

Host Firewall: Unknown	**IP Forwarding:** Unknown

System Accounts

Hardcoded Credentials: Unknown	**Hashing Algorithm:** Unknown

Anbes

Device Overview

Model: BF-A10	**Released:** Jun, 2020	**Price:** $49.98

FCC ID: 2AR5E-BF-A10	**Amazon:** B08BJLSY4T	**UPC:** None

Product: Not Found

Manual: https://tinyurl.com/manual-anbes

Device ID: ppsle9beda455d5244b6	**Serial:** 062592855

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: Yes	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** FC:6B:F0:57:C0:6C	**2.4GHz:** Yes	**5GHz:** No

Chipset: Hi1131	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: Yes	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11-g52cd25b-dirty	**Bootloader Access:** Password

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 1.0.0.5	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: No	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: CloudEdge	**ID:** com.cloudedge.smarteye

Tested Version: 3.0.5	**Released:** 07/16/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: No	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 1883	**Encryption:** No

Anran

Device Overview

Model: AR-W620	**Released:** Oct, 2020	**Price:** $56.69

FCC ID: 2AZUX-S02	**Amazon:** B06XQ5P3VP	**UPC:** None

Product: https://anran-cctv.com/products

Manual: https://fccid.io/2AZUX-S02/User-Manual/User-manual-5247067.pdf

Device ID: SSAC-038345-BCAFC	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3516 EV300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q128SIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** E0:09:BF:67:78:81	**2.4GHz:** Yes	**5GHz:** No

Chipset: MT7601U	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** Yes

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: Yes	**MAC:** 00:EF:69:E9:A3:C8

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** Password

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** No

User Can Request Update: No	**User Can Manually Install:** Yes

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: CamHi	**ID:** com.hichip

Tested Version: 7.0.0	**Released:** 08/03/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** No	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.9.37	**Date:** 12/07/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: ipc_server	**RELRO:** Partial	**Canary:** Yes	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** md5crypt

Aqara

Device Overview

Model: CH-H01	**Released:** Jul, 2020	**Price:** $69.99

FCC ID: 2AKIT-G2H	**Amazon:** B08F2DBP3Y	**UPC:** 192784000403

Product: https://www.aqara.com/en/g2h_camera_hub.html

Manual: https://tinyurl.com/manual-aqara

Device ID: N/A	**Serial:** 450/A112092400029

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** Yes

Core Hardware Components

System on Chip (SoC)

Chipset: MSC316DC	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: MX25L25645G	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 54:EF:44:CC:B4:6A	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188EUS	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2015.01	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** Yes

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: No	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Aqara Home	**ID:** com.lumiunited.aqarahome.play

Tested Version: 2.3.13	**Released:** 08/03/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-16 characters (3 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 47838	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 1883	**Encryption:** No

Linux-specific Details

Kernel Overview

Kernel: 3.18.30	**Date:** 09/12/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: camera	**RELRO:** No	**Canary:** Yes	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** Yes	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Conico

Device Overview

Model: ZS-GX3S	**Released:** Jun, 2020	**Price:** $55.99

FCC ID: 2AT5D-ZS-GX5	**Amazon:** B08C2HSNHJ	**UPC:** None

Product: https://www.conico.com/conico-b32-wire-free-battery-outdoor-camera.html

Manual: https://fccid.io/2AT5D-ZS-GX5/User-Manual/User-Manual-4385544.pdf

Device ID: 1007736445	**Serial:** 63916679

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 54:F1:5F:35:F1:98	**2.4GHz:** Yes	**5GHz:** No

Chipset: Hi3861V100	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** WLAN	**Other Baud Rate:** 115200

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** Unknown	**Bootloader Access:** No

OS Access

Auto-login: No	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 5.0.1.3	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: No	**Hash Verification:** No	**Signed Image:** No

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: CloudEdge	**ID:** com.cloudedge.smarteye

Tested Version: 3.0.5	**Released:** 07/16/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: No	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 8090	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** Openresty

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 1883	**Encryption:** No

DCT

Device Overview

Model: CG1	**Released:** Aug, 2020	**Price:** $63.99

FCC ID: 2AXBN-CG1	**Amazon:** B08F3CVP38	**UPC:** None

Product: Not Found

Manual: https://fccid.io/2AXBN-CG1/User-Manual/User-Manual-4884001.pdf

Device ID: ea815b939eb0bb65	**Serial:** AIC7FXUEGUN7015

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH128AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: No	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 7C:25:DA:29:C3:15	**2.4GHz:** Yes	**5GHz:** No

Chipset: 3131A-S	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** No

OS Access

Auto-login: N/A	**Login Prompt:** Yes	**Boot Output:** Partial	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 3.2.3	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** Yes

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: VicoHome	**ID:** com.smartaddx.vicohome

Tested Version: 2.4.0.1669(e1d2e9)	**Released:** 07/23/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 8+ characters (3 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Ecobee

Device Overview

Model: EBSCV01	**Released:** Apr, 2020	**Price:** $99.99

FCC ID: WR974100118120	**Amazon:** B087D6DRCC	**UPC:** 627988030005

Product: https://www.ecobee.com/en-us/cameras/smart-camera-with-voice-control/

Manual: https://m.media-amazon.com/images/I/918quE8iHVL.pdf

Device ID: 231f3873-9e24-5960-9c19-f2e996956660	**Serial:** 711656843203

Vendor Security Assertions

Security Policy: https://hackerone.com/ecobee

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: MT8183	**Processor:** ARM Cortex-A73	**Architecture:** 64-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: KLM4G1FETE	**Type:** eMMC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** N/A	**Sensitive Data Cleared:** N/A

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: DC Barrel	**Power Delivery:** Yes	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: No	**Media Obfuscated:** N/A	**Format:** N/A

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 44:61:32:13:41:1C	**2.4GHz:** Yes	**5GHz:** Yes

Chipset: MT7658CSN	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: Yes	**Version:** 5	**Manual Pairing:** No	**PIN Required:** No

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: No	**Baud Rate:** N/A	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** Unknown	**Bootloader Access:** N/A

OS Access

Auto-login: N/A	**Login Prompt:** N/A	**Boot Output:** N/A	**Secrets in Output:** N/A

Firmware

Operating System (OS) Overview

Type: Yocto Linux	**Version:** 13.0.0	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** EXT4

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** Yes

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** No

Transit Encryption: Yes	**SSL Labs Score:** A	**Authentication:** Yes

Companion Mobile Application

Application Overview

Name: Ecobee	**ID:** com.ecobee.athenamobile

Tested Version: 8.15+141020	**Released:** 08/22/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8+ characters

Two-Step Authentication:	***Available:*** Yes	***Required:*** Yes

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 33107	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** Unknown

Brute Force Protection: Unknown	**Banner:** None

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.4.146	**Date:** Unknown	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** Unknown

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: selene	**RELRO:** Partial	**Canary:** No	**NX:** Yes

Symbols: Present	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: No	**Hashing Algorithm:** N/A

Eversecu

Device Overview

Model: Outdoor Wireless Camera	**Released:** Sep, 2020	**Price:** $56.99

FCC ID: Not Found	**Amazon:** B08J46GGXQ	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: 4ZH6SVN5AKEGVQAIK5OQ	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: USB C	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** FC:6B:F0:8D:BD:F0	**2.4GHz:** Yes	**5GHz:** No

Chipset: Hi1131	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** Yes

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** No

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Partial	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 3.2.3	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: i-Cam+	**ID:** cn.ubia.icamplus

Tested Version: 1.1.17	**Released:** 07/02/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-32 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Feit Electric

Device Overview

Model: CAM/PAN/WIFI	**Released:** Nov, 2020	**Price:** $51.21

FCC ID: SYW-CAMPANWIFI	**Amazon:** B08P42BKGG	**UPC:** 017801722208

Product: https://www.feit.com/product/indoor-pan-tilt-smart-wi-fi-camera/

Manual: https://tinyurl.com/manual-feitelectric

Device ID: N/A	**Serial:** 063546207

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: AK3918EN080	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** DC:29:19:C6:DC:E7	**2.4GHz:** Yes	**5GHz:** No

Chipset: ATBM60321	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2013.10.0-AK_V3.0.07	**Bootloader Access:** No

OS Access

Auto-login: N/A	**Login Prompt:** No	**Boot Output:** Partial	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Anyka Linux	**Version:** 1.1.12	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** CramFS

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Feit Electric	**ID:** com.feit.smart

Tested Version: 3.0.9	**Released:** 07/28/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 3.4.35	**Date:** 01/21/2021	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** No

Binary Hardening

Sample: ppsapp	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** sha512

HeimVision

Device Overview

Model: Protect D1	**Released:** Jul, 2020	**Price:** $55.99

FCC ID: 2AWRR-PRD	**Amazon:** B08DKX6NPH	**UPC:** None

Product: https://www.heimvision.com/products/ptz-outdoor-security-camera

Manual: https://fccid.io/2AWRR-PRD/User-Manual/User-Manual-5283390.pdf

Device ID: AJ0806010200008759003g	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: GK7205	**Processor:** ARM 1176ZJFS	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 68:88:C9:44:70:6B	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: Yes	**MAC:** 3C:97:0E:22:E1:20

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2012.10	**Bootloader Access:** Yes

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Yes	**SSL Labs Score:** B	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: HeimLink	**ID:** com.vantop.heimlink

Tested Version: 4.1073.0.8880	**Released:** 06/11/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** Yes	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 6-26 characters (3 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** Ginatex-HTTPServer

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** No	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.4.43	**Date:** 09/15/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: sensordetect	**RELRO:** No	**Canary:** No	**NX:** Yes

Symbols: Present	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Jennov

Device Overview

Model: A90WT20-1-FAS-32	**Released:** Apr, 2020	**Price:** $65.50

FCC ID: Not Found	**Amazon:** B087BG2VQX	**UPC:** None

Product: Not Found

Manual: https://jennov.cn/wp-content/uploads/2021/05/T-Series-Manual.pdf

Device ID: SSAA-244060-ABAEA	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3516 EV200	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH128AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: No	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 7C:A7:B0:B8:08:E1	**2.4GHz:** Yes	**5GHz:** No

Chipset: MT7601U	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** Yes

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: Yes	**MAC:** 00:15:CD:D7:6F:92

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** Password

OS Access

Auto-login: No	**Login Prompt:** Yes	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** Yes	**Filesystem:** JFFS2

Firmware Updates

Update Support: No	**Notify User:** N/A	**Force Update:** N/A

User Can Request Update: N/A	**User Can Manually Install:** N/A

Firmware Security

Update Encrypted: N/A	**Hash Verification:** N/A	**Signed Image:** N/A

Transit Encryption: N/A	**SSL Labs Score:** N/A	**Authentication:** N/A

Companion Mobile Application

Application Overview

Name: CamHi	**ID:** com.hichip

Tested Version: 7.0.0	**Released:** 08/03/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** N/A

Two-Step Authentication:	***Available:*** N/A	***Required:*** N/A

Default Device Login: Yes	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 80	**Encryption:** No	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** None

Streaming Service

Protocol: RTSP	**Port:** 554/TCP	**Encryption:** No	**Authentication:** No	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.9.37	**Date:** 05/21/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: ipc_server	**RELRO:** Partial	**Canary:** Yes	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** md5crypt

LaView

Device Overview

Model: LV-PWR12W	**Released:** Jul, 2020	**Price:** $49.99

FCC ID: 2APD7-R9820	**Amazon:** B08F27MWVC	**UPC:** 192728011564

Product: https://www.laviewsecurity.com/r12-pt-wifi-outdoor-camera.html

Manual: https://tinyurl.com/manual-laview

Device ID: eb067ff5fe215963a8kv0a	**Serial:** 876200801X02604

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: RTS3903N	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** No	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64JVSIQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Hard Wired	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** FC:6B:F0:6F:BD:2D	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: Yes	**MAC:** 5E:19:47:86:0F:E1

Serial Console

UART Overview

UART: No	**Baud Rate:** N/A	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2014.01-v1.2	**Bootloader Access:** N/A

OS Access

Auto-login: N/A	**Login Prompt:** N/A	**Boot Output:** N/A	**Secrets in Output:** N/A

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: LaView	**ID:** com.laview.smart

Tested Version: 1.0.8	**Released:** 08/20/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters (2 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** No

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

Linux-specific Details

Kernel Overview

Kernel: 3.10.2	**Date:** 06/08/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: dgiot	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

Mascarry

Device Overview

Model: A4	**Released:** Jul, 2020	**Price:** $50.99

FCC ID: 2AUAU-A4	**Amazon:** B08CVPYCPR	**UPC:** None

Product: Not Found

Manual: https://fccid.io/2AUAU-A4/User-Manual/User-Manual-4989154.pdf

Device ID: N/A	**Serial:** 180020A02152

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Ingenic T21	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: XT25F128B	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: Yes	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** FC:CD:2F:30:9A:BF	**2.4GHz:** Yes	**5GHz:** No

Chipset: XR871	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: No	**Baud Rate:** N/A	**Other UART:** WLAN	**Other Baud Rate:** 115200

Headers Soldered: Yes	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2013.07	**Bootloader Access:** N/A

OS Access

Auto-login: N/A	**Login Prompt:** N/A	**Boot Output:** N/A	**Secrets in Output:** N/A

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Yes	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Adorcam	**ID:** com.xm.adorcam

Tested Version: 1.4.25	**Released:** 08/12/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 1883	**Encryption:** No

Linux-specific Details

Kernel Overview

Kernel: 3.10.14	**Date:** 07/15/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** No

Binary Hardening

Sample: sample-xmbakipc	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Unknown

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** None

Moonxiao

Device Overview

Model: Robot	**Released:** Sep, 2020	**Price:** $56.99

FCC ID: Not Found	**Amazon:** B08H8P4RTT	**UPC:** None

Product: Not Found

Manual: Not Found

Device ID: 25988288	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: RTS3905N	**Processor:** MIPS	**Architecture:** 32-bit MIPS

MMU Provided: Yes	**Crypto Support:** No	**Hardware PRNG:** No

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 40:AA:56:78:74:50	**2.4GHz:** Yes	**5GHz:** No

Chipset: S9083H	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2014.01-v1.2	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** Yes	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Yes	**Hash Verification:** Yes	**Signed Image:** No

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Yoosee	**ID:** com.yoosee

Tested Version: 00.46.00.69	**Released:** 02/22/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-30 characters (2 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: RTSP	**Port:** 554/UDP	**Encryption:** No	**Authentication:** Yes	**LED:** No

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 3.10.27	**Date:** 12/17/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** N/A

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: ipc	**RELRO:** No	**Canary:** No	**NX:** No

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** None

Reolink

Device Overview

Model: Lumus	**Released:** Mar, 2020	**Price:** $49.99

FCC ID: 2A7V-1909A	**Amazon:** B08628J862	**UPC:** None

Product: https://reolink.com/us/product/reolink-lumus/

Manual: https://fccid.io/2AL7V-1909A/User-Manual/User-Munaul-4670555.pdf

Device ID: 95270001RWPYKSXE	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Star SSC323	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q127CSIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: No	**Power Delivery:** N/A	**Mounts Storage:** N/A	**Debug Mode:** N/A

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 40:AA:56:53:AD:81	**2.4GHz:** Yes	**5GHz:** No

Chipset: MT7601UN	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2015.01	**Bootloader Access:** No

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** No	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** No

User Can Request Update: No	**User Can Manually Install:** Yes

Firmware Security

Update Encrypted: No	**Hash Verification:** No	**Signed Image:** No

Transit Encryption: Yes	**SSL Labs Score:** B	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Reolink	**ID:** com.mcu.reolink

Tested Version: 4.27.1.0	**Released:** 08/14/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8+ characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.9.84	**Date:** 09/06/2019	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: dvr	**RELRO:** Partial	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 1

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** descrypt

StartVision

Device Overview

Model: L-18	**Released:** Jul, 2020	**Price:** $65.99

FCC ID: Not Found	**Amazon:** B08DXQXSQF	**UPC:** None

Product: http://www.startvision.cn/index.php?id=107

Manual: Not Found

Device ID: ebed7d86eac154d1bfsaks	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH64AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: Yes	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 7C:25:DA:0C:BD:03	**2.4GHz:** Yes	**5GHz:** No

Chipset: 3131A-S	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: Yes	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Partial	**Secrets in Output:** Yes

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 3.2.3	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Smart Life	**ID:** com.tuya.smartlife

Tested Version: 3.29.5	**Released:** 07/31/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** Yes	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

TP-Link

Device Overview

Model: EC70	**Released:** Sep, 2020	**Price:** $49.99

FCC ID: TE7KC115	**Amazon:** B08GHX9G5L	**UPC:** 840030701924

Product: https://www.kasasmart.com/us/products/security-cameras/kasa-spot-pan-tilt-ec70

Manual: https://tinyurl.com/manual-tplink

Device ID: N/A	**Serial:** 220C6H0002366

Vendor Security Assertions

Security Policy: https://www.tp-link.com/us/press/security-advisory/

Vendor Security Claims:	***On Box:*** Yes	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: QH128AHIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** No	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 28:EE:52:97:72:FA	**2.4GHz:** Yes	**5GHz:** No

Chipset: RTL8188FTV	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: No	**Temporary AP Pairing:** Yes	**Temporary AP Password:** No

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: Linux	**Version:** N/A	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** Yes	**Filesystem:** SquashFS

Firmware Updates

Update Support: Yes	**Notify User:** Yes	**Force Update:** Yes

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: No	**Hash Verification:** No	**Signed Image:** Yes

Transit Encryption: No	**SSL Labs Score:** N/A	**Authentication:** No

Companion Mobile Application

Application Overview

Name: Kasa Smart	**ID:** com.tplink.kasa_android

Tested Version: 2.33.1.998	**Released:** 08/05/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 8-32 characters (3 classes)

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Yes

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: 10443	**Encryption:** Yes	**Authentication:** Yes	**Session Timeout:** No

Brute Force Protection: No	**Banner:** Streamd,

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

Linux-specific Details

Kernel Overview

Kernel: 4.9.37	**Date:** 07/31/2020	**IMA Used:** No

Signed Modules: No	**KASLR Used:** No	**Secure Boot Used:** No

Filesystem Access Controls

Discretionary Appropriate: No	**Mandatory (MAC) Used:** No

Process Management

Most Root: Yes	**cgroups:** No	**seccomp:** No	**Watchdog:** Yes

Binary Hardening

Sample: iot-client	**RELRO:** Partial	**Canary:** No	**NX:** Yes

Symbols: Removed	**PIE:** No	**Fortify:** No	**ASLR:** Mode 2

Network Security

Host Firewall: No	**IP Forwarding:** No

System Accounts

Hardcoded Credentials: Yes	**Hashing Algorithm:** None

Vacos

Device Overview

Model: Vacos Cam	**Released:** May, 2020	**Price:** $99.99

FCC ID: 2AKL2K44IPC	**Amazon:** B0888DPKFT	**UPC:** None

Product: https://www.vacos.com/products/vacos-cam

Manual: https://cdn.vacos.com/wp-content/uploads/manual/Vacos-Cam-User-Manuals.pdf

Device ID: 7a31f01c7f80d1302d5f31349b094d21	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v300	**Processor:** ARM Cortex-A7	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: Yes	**TPM Available:** Yes

Flash Memory

Chipset: 25Q128JVSQ	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** N/A	**Sensitive Data Cleared:** N/A

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: No	**Media Obfuscated:** N/A	**Format:** N/A

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** AC:64:CF:D7:98:7A	**2.4GHz:** Yes	**5GHz:** No

Chipset: 3131A-S	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2016.11	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 3.2.2	**Encrypted at Rest:** No

Flash Dump Acquired: Yes	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No	**Force Update:** No

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Yes	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Vacos	**ID:** com.anke.video

Tested Version: 1.0.3.6	**Released:** 04/17/2021	**Tuya-based:** No

Hardening

Sensitive Data Protected: No	**MITM Prevention:** No	**Root Detection:** No

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** Yes	***Required:*** Yes

Default Device Login: No	**All HTTPS API Calls:** No

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: No	**Port:** N/A	**Encryption:** N/A

WOHOME

Device Overview

Model: LY-138	**Released:** Jul, 2020	**Price:** $53.99

FCC ID: 2AFCB-LY138	**Amazon:** B086ZRR76G	**UPC:** None

Product: https://wohomeshop.com/products/smart-home-security-camera

Manual: https://fcc.report/FCC-ID/2AFCB-LY138/4795137.pdf

Device ID: eb836e4af55db33e26mvdp	**Serial:** None

Vendor Security Assertions

Security Policy: Not Found

Vendor Security Claims:	***On Box:*** No	***In Manual:*** No

Core Hardware Components

System on Chip (SoC)

Chipset: Hi3518E v200	**Processor:** ARM926EJ-S	**Architecture:** 32-bit ARM

MMU Provided: Yes	**Crypto Support:** Yes	**Hardware PRNG:** Yes

Secure Boot Available: No	**TPM Available:** Yes

Flash Memory

Chipset: 25Q64FWSIG	**Type:** SOIC

Physical Security

Factory Reset

Documented Feature: Yes	**SD Card Cleared:** No	**Sensitive Data Cleared:** No

Tamper Evident

External: No	**Internal:** No

External Interfaces

USB Usage

Type: Micro B	**Power Delivery:** Yes	**Mounts Storage:** No	**Debug Mode:** No

Removable Media

Type: MicroSD	**Media Obfuscated:** Yes	**Format:** FAT 32

Network Interfaces

Wi-Fi

Available: Yes	**MAC:** 7C:25:DA:61:AC:71	**2.4GHz:** Yes	**5GHz:** No

Chipset: 3131A-S	**WPA3 Support:** No	**WPS Support:** No

QR Pairing: Yes	**Temporary AP Pairing:** No	**Temporary AP Password:** N/A

Bluetooth

Available: No	**Version:** N/A	**Manual Pairing:** N/A	**PIN Required:** N/A

Ethernet

Available: No	**MAC:** N/A

Serial Console

UART Overview

UART: Yes	**Baud Rate:** 115200	**Other UART:** No	**Other Baud Rate:** N/A

Headers Soldered: No	**Marked in Silk Screen:** No

Bootloader Overview

Type: U-Boot	**Version:** 2010.06	**Bootloader Access:** Yes

OS Access

Auto-login: Yes	**Login Prompt:** N/A	**Boot Output:** Yes	**Secrets in Output:** No

Firmware

Operating System (OS) Overview

Type: LiteOS	**Version:** 1.4.6	**Encrypted at Rest:** No

Flash Dump Acquired: No	**Filesystem Scraped:** N/A	**Filesystem:** JFFS2

Firmware Updates

Update Support: Yes	**Notify User:** No Update Found	**Force Update:** No Update Found

User Can Request Update: Yes	**User Can Manually Install:** No

Firmware Security

Update Encrypted: Unknown	**Hash Verification:** Unknown	**Signed Image:** Unknown

Transit Encryption: Unknown	**SSL Labs Score:** Unknown	**Authentication:** Unknown

Companion Mobile Application

Application Overview

Name: Tuya Smart	**ID:** com.tuya.smart

Tested Version: 3.30.0	**Released:** 08/08/2021	**Tuya-based:** Yes

Hardening

Sensitive Data Protected: Yes	**MITM Prevention:** Yes	**Root Detection:** Yes

Service Security

Password Masked: Yes	**Password Policy:** 6-20 characters

Two-Step Authentication:	***Available:*** No	***Required:*** N/A

Default Device Login: No	**All HTTPS API Calls:** Unknown

Network Services

System Logins

Telnet Enabled: No	**SSH Enabled:** No	**FTP Enabled:** No

HTTP Service

Port: No	**Encryption:** N/A	**Authentication:** N/A	**Session Timeout:** N/A

Brute Force Protection: N/A	**Banner:** N/A

Streaming Service

Protocol: No	**Port:** N/A	**Encryption:** N/A	**Authentication:** N/A	**LED:** Yes

MQTT Management

Enabled: Yes	**Port:** 8883	**Encryption:** Yes

APPENDIX H: EXTRACTED DEVICE CREDENTIALS

Vendor	Use Case	Login	Password	Linux Hash
Akaso	Webserver	admin	56565099	N/A
Anran	Streaming	admin	admin	N/A
Anran	Linux	root	*(unknown)*	1ocmTTAhE$v.q2/jwr4BS.20KYshYQZ1
Anran	U-Boot	N/A	HI2105CHIP	N/A
Anran	Wi-Fi Setup	N/A	1234567	N/A
Aqara	Linux	root	*(unknown)*	qJfvIDmLC1TI6
Cellbee	Linux	root	*(unknown)*	6h78faswkipjq6ycu$IKmuaLoD6EoToDTUqIiq.p8x1nuLwdK37SPqv43jn0dU5PtSIiTrpakIfUTCuqT6YIP5hzOszFJlgu2K0Sh2K/
Didog	Linux	root	059AnkJ	FCb/N1tGGXtP6
Ecwey	Streaming	admin	admin	N/A
Ecwey	Linux	root	runtop10	7wtxBdUGBnuoY
Energizer	Linux	root	*(unknown)*	$1$12345678$CTq8UQyYrE.vbbG7E8Mtj1
Eversecu	Wi-Fi Setup	N/A	12345678	N/A
FeitElectric	Linux	root	helpme	ab8nBoH3mb8.g
FeitElectric	Linux	root	*(unknown)*	$1$12345678$CTq8UQyYrE.vbbG7E8Mtj1
FeitElectric	Linux	root	*(unknown)*	$6$4GbqAXEFqeauykeE$a6dqh2CoO6SucAplB/b4uvS5z0hN1Cb2r1pNWpsXL96vMqrrY42lFylXGNJm6RcY.3Lte/QS2.yyI4/pZDHAa1
HeimVision	Linux	root	cxlinux	yE7gW4O0CSXXg
Hongsa	Streaming	N/A	12345678	N/A
Hongsa	Linux	root	*(unknown)*	1xB/Ai9df$2mLQeRBzZu/2GHSk.TJWg1
IOIODOG	Linux	root	dgiot010	IsHLvr/zaeG2U
iSmartPet	Linux	root	*(unknown)*	$1$4K3g2.LW$uIo9nc74tYXc6f72N6nHi1

Vendor	Use Case	Login	Password	Linux Hash
iSmartPet	Linux	root	*(unknown)*	6x5I/xsyA$GnEc4Sg8tx2RJCQxWMhTtEQrid5elltlg.O24Z90/IWhlFKEssOd29Z8gUwV0bFZHX5bhTevZYaN6OxGREhVo/
Jennov	Streaming	admin	admin	N/A
Jennov	Linux	root	*(unknown)*	1ocmTTAhE$v.q2/jwr4BS.20KYshYQZ1
Jennov	U-Boot	N/A	HI2105CHIP	N/A
Jennov	Wi-Fi Setup	N/A	1234567	N/A
Kami Baby	Linux	root	*(blank)*	N/A
LaView	Linux	root	dgiot010	IsHLvr/zaeG2U
Mascarry	Linux	root	*(blank)*	N/A
Moonxiao	Linux	root	*(blank)*	N/A
Pambrum	Streaming	N/A	123456	N/A
Pambrum	Linux	root	*(unknown)*	1ouLOV500$zvYRvG33R/lxTS.9Gpz5H1
PetSitter	Linux	root	*(unknown)*	1RYIwEiRA$d5iRRVQ5ZeRTrJwGjRy.B0
PetSitter	Linux	root	*(unknown)*	$6$0E8/0opc$yfESwbvIce8PIEb3fCgH1kRpISzA2ffyv9VfdeM3wadmKyLfLXgNlyH3TafXvugdqPevBgE.3EZtGnP.KZZug.
Reolink	Linux	root	*(unknown)*	qdGt8T0XjiWXI
Reolink	Streaming	admin	*(blank)*	N/A
Sense-U	Linux	root	*(unknown)*	1o9G00T3j$AZyzLco30lxv/GpgKz7sZ1
Swept Supplies	Streaming	N/A	6666	N/A
TP-Link	Linux	root	*(blank)*	N/A
VicZone	Device Setup	*(variable)*	8888	N/A
VicZone	Linux	root	runtop10	7wtxBdUGBnuoY
VTech	GPG Keyring	N/A	vtechhome	N/A
VTech	Linux	root	*(unknown)*	Jv12S6L/lUMa2
Wuuk	Linux	root	xmitech	iWK.dK9N9ei7g

APPENDIX I: ASSESSMENT-TRACKING MECHANISM CONTROL TEST MATRIX

Description	Evidence Needed	Total Controls
Determine if running system services are necessary and/or insecure and at what privilege level they are started	Verification that system services are necessary for functionality, using secure protocols and least privilege	16
Determine the location of sensitive data types (e.g., passwords, keys, API tokens, PII) that are being stored (e.g., flash, USB, SD) and their use of encryption	Inventory all the sensitive data on the device and what data security controls are in place for each type	9
Determine if vulnerabilities exist in ecosystem services that allow an attacker to spoof as another user to manipulate resources against a target (e.g., IDOR)	Analysis of application security, especially for web & system services, whether local or cloud hosted for usage	10
Determine if the firmware contains any debug tooling, unstripped binaries, or other artifacts that should have been removed before shipping the firmware	Binaries on filesystem have been stripped and no manufacture debugging tools are still available	3
Determine if physical ports are enabled (e.g., JTAG, UART, USB), and if so, do they have protection from direct usage (e.g., logins) by a local attacker	Verify if any physical debug ports are available and their individual security controls to prevent direct use	9
Determine if a hardware root of trust is used for storing cryptographic key material for various device operations, such as firmware verification or mutual TLS use cases	Verification that hardware-backed cryptographic keys are being used	15
Determine if secure boot is available on the hardware, that is enabled, and that boot configuration is locked, with each stage validated and chained	Verification that Secureboot is enabled, and the boot configuration is locked with each stage validated and chained	10
Determine if binary hardening techniques have been applied to custom device system services to provide resilience against common attacks (e.g., overflows)	Verification that common binary hardening compilation flags were used on the device's local custom software	6

Description	Evidence Needed	Total Controls
Determine if local logs contain sensitive information (e.g., passwords, keys, PII) and that the bootloader output also does not contain these	Verification that logs and bootloader output are free from any secrets or other sensitive data	2
Determine if any device or cloud services use generic credentials (e.g., default, hardcoded, static API tokens) and have been generated uniquely when appropriate for new users of a device each time it is factory reset	Verification that credentials can be changed and that appropriate API tokens & private keys are unique between factory resets	16
Determine if a unique device identifier exists such that it can establish trust to the IoT ecosystem (e.g., certificate, UUID) that reliably distinguishes it from other devices, and is tamper resistant (e.g., part of a chip)	Verification that a unique device identifier exists that is verifiable, or at least not able to be brute forced, and tamper resistant via hardware backing	12
Determine if strong authentication (e.g., certificates, OTP, SMS, push, U2F, webauthn, etc.) are used for all authentication interfaces with machines or users	Verification that some form of strong authentication is found for all user-to-device and device-to-device workflows	6
Determine if primary authentication occurs via passwords or with certificates in backend workflows	Verification of how device-to-device workflows authenticate automatically	1
Determine if sensitive data (e.g., passwords, keys, PII) are removed fully from a device when it follows a factory reset process	Verification that sensitive data that was placed on the device during testing is not still present after a factory reset	6
Determine where cryptography is used for the device & ecosystem and evaluate if the configuration (e.g., ciphers, key sizes, revocation) and libraries are appropriate	Verification of each primary use case of cryptography, including revocation, key sizes, cipher suites, protocols, and libraries	15
Determine where randomness inputs are used for the core functionality of the device and evaluate if the sources of that randomness are appropriate	Verification that usage of randomness (e.g., /dev/random, /dev/urandom) are appropriate for the use cases	3
Determine if the bootloader will allow booting from an external media source (e.g., USB, SD Card) or network	Verification that code will not be booted via an external media source	1

Description	Evidence Needed	Total Controls
Determine if the firmware is encrypted and additional persistent storage is stored on an encrypted volume	Verification that firmware is encrypted, and other persistent data is stored within an encrypted volume	5
Determine if the operating system is using reasonable security configuration across core components and have updated patching applied for major services/kernel	Verification that the operating system does not have any fundamental security issues and those patches are applied	5
Determine if ASLR and/or DEP are enabled for the OS	Verification that the operating system supports ASLR and DEP for binaries	2
Determine if RAM scrambling is used by the hardware and that MMU is present to prevent bad reads	Verification that RAM scrambling and MMU is a supported by the hardware	4
Determine if IMA is in use by the operating system	Verification that IMA is being used	1
Determine if applications are running in containers	Verification that applications run using a container context (e.g., LXC, Docker)	1
Determine if Linux is using kernel namespaces	Verification that namespaces are used	1
Determine if cgroups are used for critical applications	Verification that critical applications are using cgroups in their execution	1
Determine if kernel capabilities are reduced for critical applications	Verification that capabilities are not the default for critical applications	1
Determine if seccomp BPF is being used for applications	Verification that seccomp is present for running processes	1
Determine if mandatory access controls are being used	Verification that a MAC technology is enabled with processes using it	4
Determine if OTA updates are supported outside of core firmware updates for the device	Verification that OTA updates exist outside of just firmware updates	1
Determine if device updates will be automatically installed on a pre-defined schedule/cadence	Verification that updates available will install on a specific timeline without requiring user intervention to achieve	3
Determine if firmware updates must be signed and have that signature verified before updating, without risk of a TOCTOU abuse case	Verification that updates must be cryptographically signed and that is verified before the update is installed, without any TOCTOU abuse potential	11

Description	Evidence Needed	Total Controls
Determine if firmware updates will change a user's security settings without their intervention	Verification that previously set security relevant configurations are not being overwritten after an update is applied	1
Determine if firmware can be rolled back to a previous version, even if it has been signed and is valid otherwise	Verification that an earlier, valid firmware cannot overwrite a newer, installed version of the firmware	2
Determine if a failed firmware update will revert to a previous, known good installation automatically	Verification that a failed firmware installation will go back to a known good state from the last version	4
Determine if firmware updates come from a server that is authenticated before attempting to download it	Verification that a server verification (e.g., pinning keys, mutual TLS) occurs before firmware will be downloaded	1
Determine if only required kernel modules are in use and that they have been cryptographically signed/verified	Verification that kernel modules used have a clear purpose for device function and they have been signed/verified	4
Determine if network and intra-device communications are using appropriate cryptography and protocols	Verification that network and device communications are being encrypted	14
Determine if certificates are validated (e.g., expiration, hierarchy, issuer, etc.), pinning occurs when relevant, and they are automatically refreshed as necessary	Verification that certificate meta data are validated by applications for their validity & hierarchy and use pinning when appropriate for device function, and they are refreshed when expired	9
Determine if MQTT usage restricts publishing and/or subscribing to only valid devices and services	Verification that MQTT use will not allow for publication or subscriptions by unauthorized devices/services	2
Determine if Bluetooth usage is secured (e.g., restrict pairing, non-generic, six-digit PINs, modern protocol) and disabled when not necessary for device functionality	Verification that a modern version of Bluetooth is used, without a generic PIN (>=six digits), and discover/pairing cannot be done at anytime	9

Description	Evidence Needed	Total Controls
Determine if Wi-Fi usage is secured (e.g., non-generic passphrase, modern protocol) and disabled when not necessary for device functionality, without WPS	Verification that Wi-Fi is at least WPA2, requires a custom passphrase, that WPS is disabled, and AES-CCMP used	7
Determine if cryptographic functions are occurring using hardware-backed technologies	Verification of cryptographic support with the hardware for key functionality	1
Determine if physical security decisions were made to slow down attackers (e.g., no silkscreen ports, blow security fuses, headers not present if not necessary)	Verification that debugging headers are not present, silkscreens are not present, and that security fuses are blown	3
Determine if hardware has physical security protection (e.g., anti-glitching) features built it to stop attackers	Verification of hardware features that may have physical abuse prevent	5
Determine if hardware has tamper-evident measures	Verification of tamper-evident measures (e.g., stickers, labels) on components (e.g., shell, chips)	3
Determine if a CPU watchdog is available and enabled	Verification of a CPU watch dog being present and enabled for the device	2
Determine if the filesystem has appropriate discretionary access controls	Verification that files, folders, devices, etc. have appropriate DAC permissions	2
Determine if root access is allowed by the CLI	Verification that root access is disabled for all CLI access (e.g., UART, SSH)	1
Determine if user sessions are automatically timed out or maximum lifetimes can be controlled for users	Verification that an authenticated session will automatically be terminated after a defined period	3
Determine if network filtering (e.g., firewall) is enabled	Verification that a host-based firewall is running (e.g., iptables) and configured	3
Determine if packet forwarding is enabled	Verification that packet forwarding is disabled on network interfaces	1
Determine if initial pairing (e.g., WiFi, Bluetooth) has a way to require physical possession exists for the device	Verification that any initial pairing process will need some sort of secret that is available only to a physical device owner with it in their possession	1

Description	Evidence Needed	Total Controls
Determine if credentials (e.g., Wi-Fi, user's passwords) must change after initial pairing occurs with defaults	Verification that all credentials with a default requires a change in the normal operation of the device's use	3
Determine if after a factory reset or on first boot, the device makes clear that the firmware is out of date	Verification that a new and factory-reset device warns about a new firmware update or forces the update	1
Determine if the device has a network clock source and that it uses a secure protocol (e.g., Secure NTP) for it	Verification that Secure NTP is in use and that a clock source is set/used	1
Determine that credentials do not use a blank password, a password with a username inside of it, and meets reasonable password requirements per NIST 800-63b	Verification that a password cannot be blank, contain the associated username, and meets NIST 800-63b criteria	9
Determine if authentication interfaces mitigate against brute force attacks in some manner	Verification that brute force attacks of user credentials result in a throttle or account lockout that must be resolved	2
Determine if an anonymous or guest account is allowed	Verification that a guest or anonymous account is not available by default	2
Determine if any default accounts cannot be deleted or renamed as part of the device's configuration	Verification that all default accounts can be either deleted or renamed	1
Determine if masking is performed on password inputs	Verification that password fields will mask the input data as a user types it	3
Determine if mutual authentication (e.g., certificates) are required for administrative interfaces	Verification that administrative interfaces required mutual authentication for requests	1
Determine if mobile companion applications verify integrity of files, reinitializing them if tampered with	Verification that a tampered with mobile device file will be reinitialized	2
Determine if the device will passively record anything sensitive (e.g., audio, video) without the awareness of the end user (e.g., status message, LED light)	Verification that when audio or video is being recorded, the end-user is aware through indicator or status message	1

Description	Evidence Needed	Total Controls
Determine if web servers on the device have reduced attack surface configuration as appropriate to its use	Verification that e.g., web server banners are disabled, TRACE methods are disabled, TLS renegotiation is off	3
Determine if network and service interfaces require some sort of authentication where necessary with auditing of those actions so changes are captured	Verification that network and systems service interfaces require some form of authentication prior to interacting with sensitive data or system actions with an audit trail of those actions	7
Determine if logs are cryptographically verifiable, stored off the device, and that authentication to view must occur before log data can be reviewed	Verification that logs are being sent off the device, digitally signed or encrypted with a MAC, and only viewed when an appropriate user is logged in	3
Determine if malware or other abuse monitoring occurs and sent to a central monitoring service/provider API	Verification that a local device security service (e.g., EDR) is operational with logs being sent to a service provider	2
Determine if Zigbee usage is secured (e.g., no hardcoded keys, key rotation occurs, AES-128 keys are used, etc.)	Verification that Zigbee keys are not passed over the network and not hardcoded with AES-128 in use	4