The IoT Breaches your Household Again*

1st Davide Bonaventura
Dipartimento di Matematica e Informatica
Università di Catania
Catania, Italy
d.bonaventura@studium.unict.it
orcid.org/0009-0004-4463-7991

2nd Sergio Esposito
Information Security Group
Royal Holloway
University of London
Egham, UK
sergio.esposito.2019@live.rhul.ac.uk
orcid.org/0000-0001-9904-9821

3rd Giampaolo Bella
Dipartimento di Matematica e Informatica
Università di Catania
Catania, Italy
giamp@dmi.unict.it
orcid.org/0000-0002-7615-8643

Abstract—Despite their apparent simplicity, devices like smart light bulbs and electrical plugs are often perceived as exempt from rigorous security measures. However, this paper challenges this misconception, uncovering how vulnerabilities in these seemingly innocuous devices can expose users to significant risks. This paper extends the findings outlined in previous work, introducing a novel attack scenario. This new attack allows malicious actors to obtain sensitive credentials, including the victim's Tapo account email and password, as well as the SSID and password of her local network. Furthermore, we demonstrate how these findings can be replicated, either partially or fully, across other smart devices within the same IoT ecosystem, specifically those manufactured by Tp-Link. Our investigation focused on the Tp-Link Tapo range, encompassing smart bulbs (Tapo L530E, Tapo L510E V2, and Tapo L630), a smart plug (Tapo P100), and a smart camera (Tapo C200). Utilizing similar communication protocols, or slight variants thereof, we found that the Tapo L530E, Tapo L510E V2, and Tapo L630 are susceptible to complete exploitation of all attack scenarios, including the newly identified one. Conversely, the Tapo P100 and Tapo C200 exhibit vulnerabilities to only a subset of attack scenarios. In conclusion, by highlighting these vulnerabilities and their potential impact, we aim to raise awareness and encourage proactive steps towards mitigating security risks in smart device deployment.

Index Terms—IoT, Tp-Link, Smart Homes, Smart Devices, Smart Bulb, Smart Plug, Smart Camera, Penetration Test, Vulnerability Assessment.

I. INTRODUCTION

The digital revolution in Internet of Things (IoT) devices has led to "smart" devices becoming more and more an integral part of our daily lives. From smart home appliances to industrial sensors, IoT has unlocked a world of convenience, efficiency, and innovation. The number of IoT devices worldwide is forecast to almost double from 15.1 billion in 2020 to more than 29 billion IoT devices in 2030 (Vailshery, 2023). The interconnectedness always brings forth significant security challenges that cannot be ignored. Due to their often neglected security, IoT devices are typically preferred devices by attackers. On average, 54% of organizations experience attempted cyberattacks targeting IoT devices every week. This indicates a 41% increase in the average number of weekly attacks per organization targeting IoT devices compared to 2022 (Check Point Research, 2023).

More and more inexpensive IoT devices are designed without a security-first mindset (Amit Serper, Reuven Yakar, 2023) (Andrew Laughlin, 2020), and their long lifecycles can expose them to evolving threats for years. The consequences of inadequate IoT security can be far-reaching. A compromised IoT device not only poses a risk to the privacy and safety of users but can also serve as a gateway to launch larger-scale attacks on critical infrastructures.

We observe that usually different devices produced by the same manufacturer, belonging to the same product line, e.g. Tapo, share parts of the firmware and application protocols used for communication. Following these observations, this paper rests on the following research questions: *(i) Do IoT devices from the same vendor share similar vulnerabilities? (ii) What consequences does this have on the end user's security, privacy and safety?*

A. Contributions

To answer the research questions we chose Tp-Link's IoT ecosystem as the target. Our experiments are focused on the following Tp-Link Tapo IoT devices.

1) Tp-Link Tapo Smart Wi-Fi Light device, Multi-color (L530E) (TP-Link, 2023c), targeted by previous work, leading to the discovery of several vulnerabilities (Bonaventura. et al., 2023).
2) Tp-Link Tapo Smart Wi-Fi Light Bulb, Dimmable (L510E V2) (TP-Link, 2023b).
3) Tp-Link Tapo Smart Wi-Fi Spotlight, Multicolor (L630) (TP-Link, 2023d).
4) Tp-Link Tapo Mini Smart Wi-Fi Socket (P100) (TP-Link, 2023e).
5) Tp-Link Tapo Pan/Tilt Home Security Wi-Fi Camera (C200) (TP-Link, 2023a).

We found that the tested Tapo devices, part of Tp-Link's IoT ecosystem, use the protocols outlined in previous work (Bonaventura. et al., 2023), or its variants. Consequently, we had the intuition that all attack scenarios described in previous work, or at least some of them, could most likely be exploited across all devices in the Tp-Link IoT ecosystem.

Hence, our findings regarding the tested Tp-Link devices can be summarised as follows:

- The L510E V2 and the L630 use the same protocols as the L530E, thereby making all attack scenarios exploitable.
- Communications between the Tapo app and the C200 are secured via TLS encryption, limiting exploitation of the vulnerabilities.
- The configuration process of the P100 occurs over Bluetooth rather than Wi-Fi, restricting exploitability to attack scenarios that don't target association and configuration processes.

Additionally, we introduce a new attack scenario leveraging the first two vulnerabilities outlined in previous work (Bonaventura. et al., 2023). In this scenario, the attacker authenticates as the Tapo device to the Tapo app. As a result, the attacker can obtain the victim's Wi-Fi SSID and password, as well as her Tapo email and password.

B. Ethics and Responsible Disclosure

All experiments only involve resources owned by the authors of this work, including devices, Wi-Fi networks, accounts, emails, and passwords. No user or third-party data was accessed during the experiments.

Tp-Link acknowledged the issues we responsibly reported through their Product Security Advisory (PSA) (TP-Link, 2023). We actively collaborated with them, by testing the fixes and confirming the attack scenarios are no longer exploitable or do not give the attacker any advantage. Tp-Link confirmed that they already released the necessary fixes to address the vulnerabilities and that the changes do not affect the normal use and stability of the products.

C. Paper Summary

This document proceeds with a brief overview of relevant literature in the subsequent section (§II), followed by a concise summary of prior research (§II-A). Subsequently, the new attack scenario is explained in detail (§III). Then, for all devices covered by our study, a detailed description of the applicability or non-applicability of each attack scenario is provided(§IV). Ultimately, pertinent conclusions are derived (§V).

II. RELATED WORK

This section delves into the related work within the field of IoT security.

Nebbione et al. (Nebbione and Calzarossa, 2020) delved into popular IoT protocols for data sharing and service discovery. They underscored the security risks posed by protocol limitations, device constraints, and vulnerabilities. Their conclusion emphasizes the need for enhancing service discovery protocols, implementing end-to-end security, and raising user awareness about IoT security risks.

In the work by Yaacoub et al. (Yaacoub et al., 2023), the authors underscore the importance of implementing proactive security measures in IoT systems, and highlight the limitations of traditional security methods. Their solution involves periodic ethical hacking simulations and penetration tests across various IoT components. In conclusion, the paper advocates for continuous training for all employees to make IoT systems more secure.

Unlike similar studies often focused on individual devices, Heiding et al. (Heiding et al., 2023) conducted systematic penetration tests on 22 smart devices across different categories commonly found in connected homes. As a result, a total of 17 vulnerabilities were uncovered and published as new CVEs. These vulnerabilities could grant attackers physical access to homes, posing significant risks to residents.

In the work by Akhilesh et al. (Akhilesh et al., 2022), the authors focus on enhancing the security of smart home-based IoT devices through automated penetration testing. Manual testing of IoT devices is labour-intensive and requires in-depth knowledge. To streamline this process, authors developed an automated penetration testing framework. Five smart home IoT devices were selected for testing, and common vulnerabilities were identified. The Tp-Link devices were found to be the most vulnerable, while the Google Home Mini was the most secure. The study concludes that the framework can be used by non-experts, contributing to improved IoT security and safer smart homes.

Researchers are also exploring various approaches to enhance the security levels of the IoT. For example, Hassija et al. (Hassija et al., 2019) show how four different technologies, i.e., blockchain, fog computing, edge computing, and machine learning, can be used to increase the level of security in IoT, solving some of the main security issues present in the four layers in which an IoT application can be divided, which are sensing layer, network layer, middleware layer, and application layer. Finally, *Salah* and *Khan* (Salah and Khan, 2017) present and survey major security issues for the IoT environment and show how blockchain can solve many of them.

A. Previous Attacks on Tapo Bulbs

Previous work on Tapo L530E smart bulbs (Bonaventura. et al., 2023) delineates the communication process between Tapo devices and the Tapo app, comprising three primary macro-steps: (1) *Device Discovery* - allows the Tapo app to locate the Tapo device within the local network, and to get the Tapo device's configuration; (2) *Tapo Symmetric Key Exchange Protocol (TSKEP)* - allows the Tapo app and the Tapo device to exchange a symmetric session key; (3) *Tapo device usage* - allows the user to use the Tapo device via the Tapo app, by sending get and set messages.

Within these macro-steps, authors identify and explain four vulnerabilities:

- Vulnerability 1. *Lack of authentication of the Tapo device with the Tapo app* allows an adjacent attacker to impersonate the Tapo device with the Tapo app during the TSKEP step.
- Vulnerability 2. *Hard-coded, short shared secret* allows an adjacent attacker to obtain the secret for authentication during the *Device Discovery* phase.

- Vulnerability 3. *Lack of randomness during symmetric encryption* allows an adjacent attacker to make the AES128-CBC scheme deterministic.
- Vulnerability 4. *Insufficient message freshness* allows an adjacent attacker to replay messages both to the Tapo device and the Tapo app.

These vulnerabilites were exploited by the authors in five attack scenarios, which we hereby summarise:

- Attack Scenario 1, *Fake Bulb Discovery Messages Generation,* that allows to discover Tapo devices within the network and serve false configurations to the Tapo app.
- Attack Scenario 2, *Password Exfiltration from Tapo User Account,* that allows to get the password in cleartext of the user's Tapo account, and its associated email account in hash form.
- Attack Scenario 3, *MITM Attack with a Configured Tapo L530E,* that allows to perform a Man-in-the-Middle attack and violate the confidentiality and integrity of all messages exchanged between the Tapo app and the Tapo device. This results in the exfiltration of the Tapo account password in cleartext, and the associated email account in hash form.
- Attack Scenario 4, *Replay Attack with the Smart Bulb as Victim,* that allows to replay previously intercepted messages. If the adversary can observe the smart bulb's behaviour when the message arrives, they can infer the message's meaning and reuse it at will.
- Attack Scenario 5, *MITM Attack with an Unconfigured Tapo L530E,* that allows to perform a Man-in-the-Middle attack and intercept traffic between the Tapo app and the Tapo device during configuration. As Tapo username and password, together with the Wi-Fi SSID and Wi-Fi password are sent in Base64 encoding during configuration, the adversary is able to exfiltrate all information.

Finally, the authors conduct experiments across three different network setups, denoted as *Setup A*, *Setup B*, and *Setup C*. In Setup A, both the victim (i.e., a phone running the Tapo app) and the adversary are connected to the same network, while the Tapo device is on a separate, remote network; in Setup B, the adversary, the victim and the Tapo device are all connected to the same local network, and the Tapo device is already configured; in Setup C, the adversary keeps deauthenticating (Bellardo and Savage, 2003) the Tapo device, resetting it to the unconfigured state, until the user connects it to the adversary's Wi-Fi honeypot, thinking it's their home network.

III. BREACHING THE HOUSEHOLD AGAIN

In this section, we present a novel attack scenario, which we call *"Attack Scenario 6 - Passwords exfiltration with an unconfigured Tapo device"*, following the enumeration within previous work on Tapo devices (Bonaventura. et al., 2023). In this new attack scenario, the adversary is able to exfiltrate passwords using an unconfigured Tapo device.

The devices used during the attack are:

- A Wi-Fi switch to provide local connectivity.
- A smart bulb Tapo series L530 with Hardware Version 1.0.0 and Firmware Version 1.1.9.
- A Samsung smartphone running Android 11 and the Tapo app Version 2.8.14.
- An Ubuntu 22.04 machine with 5.15.0-47 kernel.

A. Setup D

The network configuration we use during the attack, which we call *Setup D*, for consistency with previous work (Bonaventura. et al., 2023), is as follows.

- The victim wants to associate an unconfigured Tapo device with her Tapo account.
- The Tapo app (hence, the victim) believes to be connected to the network *X* created by the Tapo device, but is actually connected to a network *Y* controlled by the attacker's Ubuntu device.

This setup requires that the Tapo device has been reset or has not been configured yet. The attacker must only be connected to the network they control, and not to the access point started by the Tapo device. The victim's Tapo app must be connected to the network controlled by the attacker. In this setup, the victim opens the Tapo application and starts the device association process. The network configuration for this setup is shown in Figure 1.
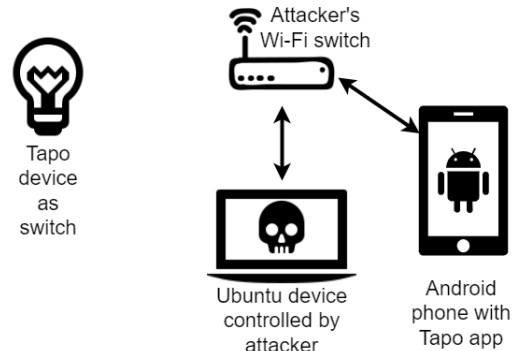

Figure 1: Setup D, network with a non-configured device.

As shown in previous work (Bonaventura. et al., 2023), the attacker can use the *Wi-Fi deauthentication attack* (Bellardo and Savage, 2003) to easily get the *Setup D* as well. Initially, the adversary can use the deauthentication attack to disconnect the Tapo device from the network to which it is connected, forcing the victim to reset it. Subsequently, after the Tapo device enters setup mode, the attacker can perform the same attack to deauthenticate the Tapo app from the network started by the Tapo device, trying to get the victim to connect to the network they control.

B. Attack Scenario 6

In this experiment, we exploited two of the four vulnerabilities, in order:

- *Vulnerability 2*, with the goal of creating fake *device discovery response*,

- *Vulnerability 1*, with the goal of authenticating as the Tapo device to the Tapo app.

The context in which we conduct the experiment is the Setup D(§III-A) previously described. The attack diagram is shown in Figure 2.
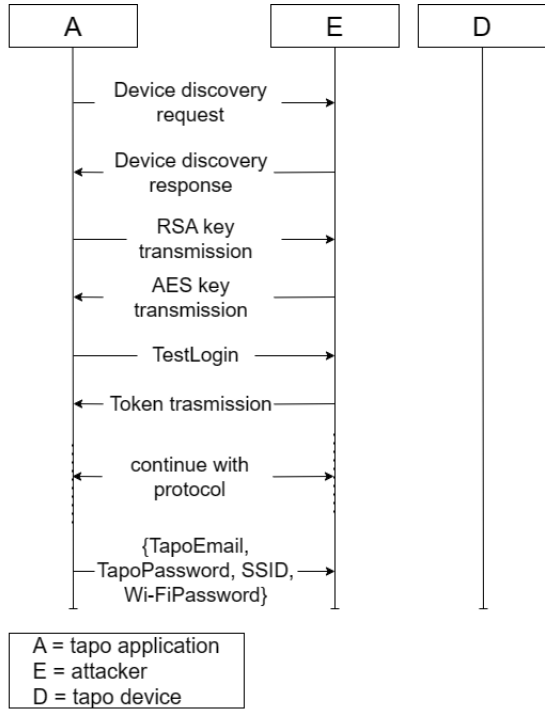

Figure 2: Sequence chart for the attack scenario 6.

The exploitation begins when the victim starts the association process within the Tapo app. In the beginning, the app starts broadcasting *device discovery request*. Hence, the attacker exploits his ability to create fake *device discovery response* to respond to various *device discovery request* from the victim. The attacker sets the response's messages fields as shown in Listing 1:

- He sets the *device_id* and *owner* fields with random hex values.
- He sets the *device_type* and *device_model* fields with the name and type of the device he wants to impersonate.
- He sets the *ip* and *port* fields to point to an adversary-controlled server.
- He sets the *factory_default* field to `true`. This is important because it allows the application to understand that the response is coming from a device not yet associated with any accounts.

Note that, differently from the *Attack Scenario 2* described in previous work (Bonaventura. et al., 2023), the attacker does not need the victim's *owner id*.

```
{
  "result": {
    "device_id": "RANDOM.HEX.VALUE",
    "owner": "RANDOM.HEX.VALUE",
    "device_type": "DEVICE.TYPE",
```

```
    "device_model": "DEVICE.MODEL",
    "IP": "ATTACKER.IP",
    "mac": "ATTACKER.PORT",
    "factory_default": true,
    "is_support_iot_cloud": false,
    "mgt_encrypt_schm": {
      "is_support_https": false,
      "encrypt_type": "AES",
      "http_port": 80
    }
  },
  "error_code": 0
}
```

Listing 1: JSON attack scenario 6

After receiving the response, the Tapo app assumes that it comes from a device that needs to be associated. Therefore, it starts the TSKEP protocol with the attacking device. Because of *vulnerability 1*, the TSKEP protocol does not give the Tapo app any evidence about the identity of the interlocutor. For this reason, the Tapo app assumes that the newly received key is shared with the device to be associated, while it is shared with the attacker instead. The attacker must then perform the association process with the Tapo app until the *set_qs_info* request. At that point, they can get the password of the victim's Tapo account and the associated email address, as well as the SSID and the password of the victim's local network.

The attack can be summarised as follows:

- The attacker gets the *Device Discovery* shared key and creates fake *device discovery response*. Therefore, the authentication of the *device discovery response* fails.
- The Tapo app executes the TSKEP protocol with the attacker instead of the Tapo device. Therefore, authentication of the Tapo device with the Tapo app fails. This results in an *integrity loss*.
- The Tapo app shares the key with the attacker, hence the distribution of the session key fails. This results in an *confidentiality loss*.
- The attacker can violate the confidentiality of the messages and get the password and the hash of the email of the victim's Tapo account as well as the SSID and the password of the victim's local network. This results in a *confidentiality loss*.

IV. IMPACT ON TARGET DEVICES

Table I provides an overview of the different versions tested for Tapo devices and the Tapo app. We tested versions of device firmwares that were supposedly vulnerable to the discovered vulnerabilities, then we tested the fixed firmwares to check if the vulnerabilities were not exploitable anymore.

A. Firmware Without Fixes

Our primary focus is to assess the impact of the identified vulnerabilities on each target device. A summary of the vulnerabilities exposed by each target device running a firmware without fixes is shown in Table II. Throughout the section, we also analyze the applicability of the attack scenarios, and we summarise the reproducible ones on each target device in Table III.

Table I: Tested versions

	Vulnerable Version	Fixed Version
L530E	1.1.9	1.2.4
L510E	1.0.8	1.1.0
P100	1.4.9 and 1.4.16	1.5.0
C200	1.1.18	-
L630	1.0.3	1.0.4
Tapo App	2.8.14 and 2.16.112	2.17.206

Table II: Vulnerabilities exposed by target devices for firmware without fixes

	Vuln. 1	Vuln. 2	Vuln. 3	Vuln. 4
L530E	🐞	🐞	🐞	🐞
L510E	🐞	🐞	🐞	🐞
L630	🐞	🐞	🐞	🐞
P100	🐞	🐞	🐞	🐞
C200	🛡	🐞	🛡	🛡

🐞 if the vulnerability is present, 🛡 otherwise.

1) Tp-Link Tapo Smart Wi-Fi Light device, Multicolor (L530E): We test an L530E with *Hardware v1.0.0* and *Firmware v1.1.9*, using a Tapo app *v2.8.14*. The smart bulb exposes all the vulnerabilities, and all *attack scenarios* are reproducible (Bonaventura. et al., 2023), including our novel *Attack Scenario 6* (§III).

2) Tp-Link Tapo Smart Wi-Fi Light Bulb, Dimmable (L510E V2): We test an L510E V2 with *Hardware v2.0* and *Firmware v1.0.8*, using a Tapo app *v2.16.112*. The Tapo L510E, for the *Device-App* communications, uses the same vulnerable protocols (§II-A) with the same security parameters used by the L530E, i.e., HTTPS protocol is not supported, CBC-AES128 bit encryption is used, and Wi-Fi is the communication channel during configuration. Therefore, this smart bulb exposes all the listed vulnerabilities, and all *attack scenarios* can be reproduced, including *Attack Scenario 6* introduced in this paper.

We hereby describe how we apply each attack scenario to the new device, highlighting any differences from previous work (Bonaventura. et al., 2023) as necessary. For newly tested

Table III: Feasibility of the Attack Scenarios (AS) on the target devices for firmware without fixes

	AS1	AS2	AS3	AS4	AS5	AS6
L530E	🐞	🐞	🐞	🐞	🐞	🐞
L510E	🐞	🐞	🐞	🐞	🐞	🐞
L630	🐞	🐞	🐞	🐞	🐞	🐞
P100	🐞	🐞	🐞	🐞	⊘	⊘
C200	🐞	🛡	🛡	🛡	🛡	🛡

🐞 if the attack scenario is feasible on the target device, 🛡 if the attack scenario is not feasible because the communication is encapsulated within a TLS channel, ⊘ if the attack scenario is not feasible because the configuration is done on the Bluetooth channel.

devices, we will refer to the L510E's behaviour as a baseline. In later sections, we will only detail Attack Scenarios (AS) that deviate from this baseline.

AS1 works with the Tapo L510E firmware tested. The key that this device uses for the Message Authentication Code is static and hardcoded, the same used by the Tapo L530E. Therefore, an attacker can create false *device discovery* messages for both the bulb and the app.

AS2 works with the Tapo L510E firmware tested. The Tapo L510E communicates using the TSKEP protocol with the Tapo app. By creating fake *device discovery response*, the attacker can impersonate the Tapo L510E, prompting the app to start TSKEP with them. This allows the attacker to get the Tapo password and the hash of the victim's Tapo email.

AS3 works with the Tapo L510E firmware tested. TSKEP lacks identity verification, enabling the attacker to perform a MITM attack on the Tapo L510E-Tapo app communication, compromising confidentiality.

AS4 works with the Tapo L510E firmware tested. The Tapo L510E accepts all messages without checking their timestamp. This allows attackers to replay sniffed messages with non-expired session keys, enabling arbitrary command execution.

AS5 works with the Tapo L510E firmware tested. During pairing, communications between the Tapo L510E and the Tapo app happen over Wi-Fi. Hence, the attacker can perform a MITM attack and hijack the association process.

AS6 works with the Tapo L510E firmware tested. During pairing, Tapo L510E and Tapo app communicate via Wi-Fi. TSKEP's identity verification vulnerability allows MITM attacks, compromising the email and password of the victim's Tapo account, as well as the SSID and password of her local network.

3) Tp-Link Tapo Smart Wi-Fi Spotlight, Multicolor (L630): We test an L630 with *Hardware v1.0* and *Firmware v1.0.3*, using a Tapo app *v2.16.112*. We confirmed this device aligns with our baseline —— mirroring the behavior of the Tapo L510E V2. Thus, it shares all listed vulnerabilities and allows reproduction of all *attack scenarios*, including the new *Attack Scenario 6* introduced in this paper.

4) Tp-Link Tapo Mini Smart Wi-Fi Socket (P100): We test a P100 with *Hardware v1.20.0* and *Firmwares v1.4.9 and v1.4.16*, using Tapo app *v2.16.112*. This device employs vulnerable protocols (§II-A), lacks HTTPS support, and uses CBC-AES128 encryption, exposing all vulnerabilities. Unlike previous devices, P100 uses Bluetooth for configuration, limiting attack scenarios to those involving already associated devices. Hence, Attack Scenarios 1 to 4 are aligned with our baseline, while Attack Scenarios 5 and 6 cannot be reproduced on Tapo P100 because the adversary is not able to perform the MITM attack during the bulb configuration process.

5) Tp-Link Tapo Pan/Tilt Home Security Wi-Fi Camera (C200): We test a C200 with *Hardware v1.0.0* and *Firmware*

v1.1.18, using a Tapo app *v2.16.112*.

Unlike the other analysed devices, the Tapo C200 supports HTTPS, utilizing TLS for TSKEP between the Tapo app and device even during configuration. This limits exposure to only *Vulnerability 2*. The use of TLS prevents message inference or traffic sniffing by requiring a valid certificate from the attacker. While TSKEP remains vulnerable to replay attacks, TLS encapsulation ensures security. Consequently, only *Attack scenario 1* can be reproduced out of six attack scenarios.

One potential attack involves downgrading the communication channel from HTTPS to HTTP. The attacker may attempt this by replying to the *device discovery requests* from the application with the same security parameters supported by the Tapo L530E, i.e., HTTPS not supported, as shown in Listing 2. However, we verified that this downgrade attack produces no results. This is because the Tapo application does not consider valid all *device discovery response* received from C200 devices that do not support HTTPS.

```
{
  "error_code": 0,
  "result": {
    "device_id": "1234...441",
    "device_name": "Tapo_Camera_E3FF",
    "device_type": "SMART.IPCAMERA",
    "device_model": "C200",
    "ip": "192.168.1.55",
    "mac": "AA-BB-CC-DD-EE-FF",
    "hardware_version": "1.0",
    "firmware_version": "1.1.18 Build 220518
        Rel.61472n(4555)",
    "factory_default": false,
    "is_support_iot_cloud": false,
    "mgt_encrypt_schm": {
      "is_support_https": false,
      "encrypt_type": "AES",
      "http_port": "Evil.tcp_port"
    }
  }
}
```

Listing 2: Attack sub-scenario 2 UDP discovery response

B. Firmware With Fixes

For each device tested, we diligently communicated the discovered vulnerabilities to Tp-Link. The responsible disclosure process enabled Tp-Link to promptly identify and address the vulnerabilities. They developed new versions of the Tapo app and the Tapo devices' firmware, implementing security updates to resolve the issues. We then actively tested the beta versions of this firmware, confirming the mitigation of potential risks arising from the vulnerabilities, and providing feedback to the manufacturer.

Although only three out of the four vulnerabilities, i.e., *Vuln. 1*, *Vuln. 3*, and *Vuln. 4*, were addressed with fixes, their absence indirectly mitigates the risk associated with the remaining vulnerability, i.e., *Vuln. 2*, making it acceptable. Therefore, even if the last vulnerability is still exposed, it would not pose a significant security risk to the end user. A summary of the vulnerabilities exposed by each target device running a firmware with fixes is shown in Table IV.

Table IV: Vulnerabilities exposed by target devices for firmware with fixes

	Vuln. 1	Vuln. 2	Vuln. 3	Vuln. 4
L530E	🛡	🐞	🛡	🛡
L510E	🛡	🐞	🛡	🛡
L630	🛡	🐞	🛡	🛡
P100	🛡	🐞	🛡	🛡
C200	-	🐞	-	-

🐞 if the vulnerability is still present, 🛡 otherwise,
- if it was not present in the unpatched firmware.

Regarding the attack scenarios, we tested all six of them using the beta version of the Tapo app, specifically *Version 2.17.206*, and the device's firmware provided by the Tp-Link. Only one of the six attack scenarios can still be reproduced, i.e., *Attack scenario 1, Fake Bulb Discovery Messages Generation*. However, the inability for the adversary to reproduce the other scenarios renders Attack scenario 1 virtually negligible in terms of risk to the victim, thus offering no advantage to the potential attacker. This observation confirms that all attack scenarios are effectively nullified, as none yields any results. A summary of the reproducible attack scenarios on each device running a firmware with fixes is shown in Table V.

Table V: Impact of the Attack Scenarios (AS) on the target devices for firmware with fixes

	AS1	AS2	AS3	AS4	AS5	AS6
L530E	🐞	🛡	🛡	🛡	🛡	🛡
L510E	🐞	🛡	🛡	🛡	🛡	🛡
L630	🐞	🛡	🛡	🛡	🛡	🛡
P100	🐞	🛡	🛡	🛡	-	-
C200	🐞	-	-	-	-	-

🐞 if the AS is feasible without benefits for the attacker,
🛡 if the AS is not feasible anymore,
- if the AS was not feasible in the unpatched firmware.

V. CONCLUSIONS

In this paper, we attempted to exploit different Tapo devices using vulnerabilities that affected the Tapo L530E smart bulb, which were found in previous work. Results show that said vulnerabilities are present and exploitable in other devices belonging to the Tp-Link ecosystem and not exclusive to a specific Tapo device. More generally, to answer our first research question, this hints at the fact that the stack of technologies underlying IoT devices is shared between devices of the same family, and that advisories published for a single device may actually be helpful to both attackers and defenders in identifying the same vulnerabilities on other devices of the same ecosystem. This is most likely not unique to the Tapo environment, but verification of this claim is left to future work.

Additionally, we expanded previous work by introducing a new Attack Scenario, which we called *"Attack Scenario*

6", and a novel network configuration to exploit the vulnerabilities, which we called *"Setup D"*. We then tested all attack scenarios on different Tapo devices, finding that they are mostly reproducible, with a few exceptions. Hence, we answer our second research question by verifying that exploitable vulnerabilities retain their potential of obtaining the Tapo account password of the victim user, even when exploited on other Tapo devices. This could allow the attacker to access the victim's account and control all associated devices. Additionally, the possibility to obtain the password of the victim's private network should not be underestimated as well, as network access can be the entry point for the attacker to execute different attacks on other devices within the network.

REFERENCES

Akhilesh, R., Bills, O., Chilamkurti, N., and Chowdhury, M. (2022). Automated penetration testing framework for smart-home-based iot devices. *Future Internet*, 14:276.

Amit Serper, Reuven Yakar (2023). 'friendlyname' buffer overflow vulnerability in wemo smart plug v2. https://sternumiot.com/iot-blog/mini-smart-plug-v2-vulnerability-buffer-overflow.

Andrew Laughlin (2020). Cheap smart plugs could expose you to hackers, or even cause a fire. https://www.which.co.uk/news/article/cheap-smart-plugs-could-expose-you-to-hackers-or-even-cause-a-fire-aMuck9K2OSYx.

Bellardo, J. and Savage, S. (2003). 802.11 {Denial-of-Service} attacks: Real vulnerabilities and practical solutions. In *12th USENIX Security Symposium (USENIX Security 03)*.

Bonaventura., D., Esposito., S., and Bella., G. (2023). Smart bulbs can be hacked to hack into your household. In *Proceedings of the 20th International Conference on Security and Cryptography - SECRYPT*, pages 218–229. INSTICC, SciTePress.

Check Point Research (2023). The tipping point: Exploring the surge in iot cyberattacks globally. https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on iot security: Application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743.

Heiding, F., Süren, E., Olegård, J., and Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, 126:103067.

Nebbione, G. and Calzarossa, M. C. (2020). Security of iot application layer protocols: Challenges and findings. *Future Internet*, 12(3).

Salah, K. and Khan, M. (2017). Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82.

TP-Link (2023). Tp-link product security advisory. https://www.tp-link.com/us/press/security-advisory/.

TP-Link (2023a). Tp-link tapo c200 - cloud camera. https://www.tp-link.com/en/home-networking/cloud-camera/tapo-c200/.

TP-Link (2023b). Tp-link tapo l510e v2 - smart bulb. https://www.tp-link.com/en/home-networking/smart-bulb/tapo-l510e/v2/.

TP-Link (2023c). Tp-link tapo l530e - smart bulb. https://www.tp-link.com/en/home-networking/smart-bulb/tapo-l530e/.

TP-Link (2023d). Tp-link tapo l630 - smart plug. https://www.tapo.com/en/product/smart-light-bulb/tapo-l630/.

TP-Link (2023e). Tp-link tapo p100 - smart plug. https://www.tp-link.com/en/home-networking/smart-plug/tapo-p100/.

Vailshery, L. S. (2023). Number of internet of things (iot) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Yaacoub, J.-P. A., Noura, H. N., Salman, O., and Chehab, A. (2023). Ethical hacking for iot: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, 3:280–308.