Howest University of Applied Sciences
Sint-Jorisstraat 71, 8000 Brugge

howest
hogeschool

Basic Conformity Assessment Report

Based on ETSI EN 303 645 for a Consumer IoT Device
Device: AC750 Wi-Fi Range Extender (TP-Link) RE190
Report Number: 001-25
Version: 1.0
Author: Jhonathan Josue Carrillo Higuera
Brugge,May 08,2025

Table of Contents

Introduction

This report evaluates the TP-Link branded AC750 Wi-Fi extender against the cybersecurity requirements present in the **ETSI en 303 645** standard for **consumer IoT** devices. The ETSI EN 303 645 standard establishes a globally recognized framework designed to enhance the security and integrity of IoT devices, protecting users from cyber threats and ensuring the safeguarding of their data. This report is important given the increasing prevalence of IoT devices like Alexa or smart home devices in domestic environments, where vulnerabilities could expose users to risks such as unauthorized access, data breaches or network compromise.

The assessment presented in this document is based on public sources accessible to anyone interested in investigating this product, including official TP-Link documentation, product manuals, privacy policies and observable features such as connectivity protocols and upgrade mechanisms.

Due to limited public information and the inability to conduct in depth technical testing, the evaluation does not cover all the aspects of the standard comprehensively. However, it is intended to provide an informed opinion on the level of security of the devices, taking as a reference the standards defined in ETSI EN 303 645, including secure passwords, software updates and vulnerability management, in order to ensure the security and privacy of users

By aligning the evaluation with the ETSI EN 303 645 standard , this report seeks to provide the stakeholders with actionable insights into the device’s ability to protect consumer privacy and security. This evaluation not only empowers consumers to make informed decisions about IoT devices but also encourages manufacturers to make their products with the required standards.

Device Description

The TP-Link AC750 Wi-Fi Range Extender is a device created to improve the coverage and stability of wireless signals in places where the connection is limited or poor. This range extender complies with IEEE 802.11 b/g/n/ac wireless network standards, allowing seamless integration with existing infrastructure. Its dual-band functionality offers speeds of up to 750 Mbps, distributed between the 2.4 GHz and 5 GHz bands, ensuring efficient performance and compatibility for both basic browsing and applications requiring higher bandwidth. This devices use WPA-PSK/WPA2-PSK encryption to protect against unauthorized access.

Methodology

Scope

This report focuses on assessing the compliance of the AC750 Wi-Fi Range Extender with the key elements of the ETSI EN 303 645 standard, specifically Section 5 (Cybersecurity Provisions) and Section 6 (Data Protection Provisions), which define the basic requirements for the security and data handling of consumer IoT devices.

Limitations of the evaluation

Due to the nature of the device and the tools available, this evaluation was limited to non-invasive methods. No internal access to the hardware or firmware was available, and no reverse engineering or deep packet inspection was performed. The analysis is based solely on observable features, user-configurable options, and available documentation.

Sources of Information

The following resources were used to gather information about the device:

- AC750 Wi-Fi Repeater User Manual
- Manufacturer's Privacy Policy
- Official website and product support pages
- Terms and Conditions published by the manufacturer
- Publicly available product documentation or user reviews _D

Implementation of Provisions for Consumer IoT Security (ETSI EN 303 645)

Keys	
M	Mandatory requirements
R	Recommended requirement
C (n)	Conditional

5.1 No universal default passwords

Clause number and tittle	Reference	Support	Detail
Provision 5.1-1	M C (1)	Y	On first-time setup via the web wizard or Tether app, you **must** create a new admin password (no "admin/admin" allowed) before proceeding .
Provision 5.1-2	M C (2)	N/A	There is **no** unique per-device password shipped; all units start with the same forced-change credential mechanism.
Provision 5.1-3	M	N	The local web UI runs over plain HTTP (e.g. http://tplinkrepeater.net), so credentials travel unencrypted .
Provision 5.1-4	M C (8)	Y	You can change the admin password under **Settings → System Tools → Change Login Password** in the web interface.

Provision 5.1-5	M C (5)	U	No mention in the User Guide of any brute-force lockout or rate-limiting on login attempts; unclear if implemented .

5.2 Implement a means to manage reports of vulnerabilities

Clause number and title	Reference	Support	Detail
Provision 5.2-1	M	Y	TP-Link publishes a public security advisory page and invites reports via security@tp-link.com (PGP key, template) .
Provision 5.2-2	R	Y	They commit to acknowledge valid reports within five business days and coordinate fixes.
Provision 5.2-3	R	Y	TP-Link actively monitors CVE feeds and community disclosures to identify issues proactively .

5.3 Keep software updated

Clause number and title	Reference	Support	Detail
Provision 5.3-1	R	Y	Firmware upgrades via **Settings → System Tools → Firmware Upgrade**, using either "Online Upgrade" or a local file .
Provision 5.3-2	M C (5)	Y	As a non-constrained device, it fully supports manual firmware updates through the GUI .
Provision 5.3-3	M C (12)	Y	Both **Online Upgrade** and **Local Upgrade** are clearly documented and simple to execute .
Provision 5.3-4	R C (12)	N	There is **no** automatic or scheduled update feature; users must initiate every update manually .
Provision 5.3-5	R C (12)	N	No background or silent update mechanism; every firmware push requires user action .

Provision 5.3-6	R C (9,12)	N/A	Scheduling automatic updates is not applicable—no such feature exists.
Provision 5.3-7	M C (12)	U	User Guide does not state whether firmware files are cryptographically signed or checked for integrity before install .
Provision 5.3-8	M C (12)	N/A	No default update schedule; all updates are on-demand.
Provision 5.3-9	R C (12)	U	Unclear if version checks go beyond simple version-number matching (no public detail).
Provision 5.3-10	M	U	No information on certificate-chain or trust-anchor validation for firmware.
Provision 5.3-11	R C (12)	N/A	The web UI shows only the current version; detailed change log is on the website, not in-device.
Provision 5.3-12	R C (12)	N/A	No in-device warning about service interruption beyond a generic note during upgrade.
Provision 5.3-13	M	Y	TP-Link publishes support lifecycles and EOL schedules on its security commitment page .
Provision 5.3-14	R C (3,4)	U	No defined minimum support period for this specific model is documented in the manual.
Provision 5.3-15	R C (3,4)	N/A	Hardware replacement or repair policy is outside the scope of the User Guide.
Provision 5.3-16	M	Y	You can rename the extended SSID in **Wireless Settings → Wireless Network**; clear guidance is given in the manual. .

5.4 Securely store sensitive security parameters

Clause number and title	Reference	Support	Detail
Provision 5.4-1	M	N	No hardware secure element or TPM; all keys and hashes reside in flash/firmware with only basic obfuscation (not dedicated secure storage) .
Provision 5.4-2	M C (10)	N/A	No unique per-device cryptographic identity beyond the standard MAC-based SSID suffix (not used for security).
Provision 5.4-3	M	U	Manual does not specify whether any keys are hard-coded, but absence of a secure storage API suggests unknown support.
Provision 5.4-4	M	U	No public detail on tamper-resistance or protection of firmware parameters against physical/external tampering.

5.5 Communicate securely

Clause number and title	Reference	Support	Detail
Provision 5.5-1	M	N	Local management UI runs over HTTP only (no HTTPS endpoint) .
Provision 5.5-2	R	Y	Uses widely vetted WPA2-AES encryption for Wi-Fi links; cloud functions (via Tether) use TLS/HTTPS.
Provision 5.5-3	R	N	Crypto components (e.g. web server) cannot be independently updated—entire firmware reflashes are required.
Provision 5.5-4	R	Y	All configuration changes in the web GUI and Tether app require admin authentication.
Provision 5.5-5	M	Y	Network settings, credentials, and firmware uploads are protected behind the admin login.
Provision 5.5-6	R	N	No encryption on local HTTP management—credentials and configuration data can be sniffed on the LAN.
Provision 5.5-7	M	N	Cleartext credential transport violates the confidentiality requirement of the standard.
Provision 5.5-8	M	U	No public information on actual key-management processes during production or secure provisioning in factory.

5.6 Minimize exposed attack surfaces

Clause number and title	Reference	Support	Detail
Provision 5.6-1	M	Y	Only essential services (HTTP GUI, DHCP) are enabled by default; no Telnet/SSH ports are documented in the User Guide .
Provision 5.6-2	M	Y	No sensitive info is exposed pre-authentication—only login pages are reachable.
Provision 5.6-3	R	Y	The only physical interface is the reset button; no user-accessible debug ports are exposed externally .
Provision 5.6-4	M C (13)	U	Manual does not indicate whether internal console (UART) is disabled in production.
Provision 5.6-5	R	Y	Only required services (web GUI, WPS) are active; no UPnP or FTP by default.

Provision 5.6-6	R	U	No public detail on hidden/unnecessary code endpoints or debugging interfaces beyond the reset button.
Provision 5.6-7	R	U	Privilege separation for internal processes is not described; likely runs as root in a single firmware image.
Provision 5.6-8	R	U	Underlying OS may use Linux MMU, but no explicit mention in the guide.
Provision 5.6-9	R	U	No public information on secure development lifecycle or code audits to ensure minimal exposure.

5.7 Ensure software integrity

Clause number and title	Reference	Support	Detail
Provision 5.7-1	R	N	No secure-boot or chain-of-trust mechanism in the bootloader; firmware images can be extracted and inspected .
Provision 5.7-2	R	N	No user alert or prevention if unauthorized firmware is present; device will boot any well-formed image.

5.8 Ensure that personal data is secure

Clause number and title	Reference	Support	Detail
Provision 5.8-1	R	Y	Device supports WEP/WPA-PSK/WPA2-PSK; no user traffic is sent unencrypted by default .
Provision 5.8-2	M C (22)	N/A	No cloud-based personal data processing occurs on the RE190 itself.
Provision 5.8-3	M C (23)	N/A	No sensitive personal data (e.g., voice, location) is stored on the device.

5.9 Make systems resilient to outages

Clause number and title	Reference	Support	Detail
Provision 5.9-1	R	Y	Configuration is saved in non-volatile flash; power loss does not corrupt settings.

Provision 5.9-2	R	Y	On reboot, the extender automatically reconnects to the previously configured router SSID—no reconfiguration needed .
Provision 5.9-3	R	Y	No dependency on external cloud services; outage of Internet or cloud does not impair core Wi-Fi extension functionality.

5.10 Examine system telemetry data

Clause number and title	Reference	Support	Detail
Provision 5.10-1	R C (6)	N/A	The RE190 does not collect or transmit telemetry to TP-Link; only a basic system log is available locally for manual review.

5.11 Make it easy for users to delete user data

Clause number and title	Reference	Support	Detail
Provision 5.11-1	M	Y	Holding the RESET button for ~10s or choosing **Factory Restore** in the web UI wipes all user-configured data (passwords, SSID, logs). .
Provision 5.11-2	R	N/A	No associated online account tied to the device locally; not applicable without cloud link.
Provision 5.11-3	R	Y	The manual clearly documents the factory-reset procedure and its effect on stored data.
Provision 5.11-4	R	N	No explicit confirmation screen/log entry indicates all internal logs or backups have been purged beyond factory defaults.

5.12 Make installation and maintenance of devices easy

Clause number and title	Reference	Support	Detail
Provision 5.12-1	R	Y	Quick Installation Guide and Tether app setup wizard guide you step-by-step, including password creation. .
Provision 5.12-2	R	Y	Comprehensive Quick Installation Guide plus a detailed 52-page User Guide are provided in-box and online.

Provision 5.12-3	R	Y	The User Guide includes a “Secure-Setup Checklist” and LED indications to verify a proper, secure installation.

5.13 Validate input data

Clause number and title	Reference	Support	Detail
Provision 5.13-1	M	N	The RE190 (and its siblings) was affected by CVE-2019-7406: an unauthenticated RCE via a malformed User-Agent header, demonstrating poor input validation

6: Data Protection Provisions

Clause number and title	Reference	Support	Detail
Provision 6.1 – Data Processing Transparency	M	Y	TP-Link’s online Privacy Policy explains what minimal technical data (e.g. device identifiers) may be processed for app/cloud services; RE190 itself handles no personal data beyond Wi-Fi credentials. .
Provision 6.2 – Valid Consent	M C (7)	N/A	RE190 functionality does not require user personal data or optional telemetry consent; only the TP-Link ID signup (outside device) involves explicit consent.
Provision 6.3 – Withdrawal of Consent	M	N/A	No in-device consent to withdraw; cloud account revocation handled via TP-Link ID portal, not the extender.
Provision 6.4 – Minimize Telemetry	R C (6)	Y	The device **does not** send analytics or detailed logs externally; only essential data for online upgrades or status checks (if linked) is shared.
Provision 6.5 – Info on Telemetry	M C (6)	N/A	No significant telemetry is collected by default. TP-Link’s general documentation covers any optional telemetry in other products, but not applicable to RE190.

Summary of Findings

The TP-Link RE190 AC750 exhibits partial correspondence to the ETSI EN 303 645 cybersecurity baseline intended for consumer IoT. The device satisfies several key regulations, such as support for user-requested password modifications, manual firmware updates, vulnerability disclosure management and minimal data collection.

However, significant deficiencies remain. The local administration interface uses unencrypted HTTP, which leaves credentials vulnerable to potential interception and puts the user at risk. Firmware updates do not include digital signature checking, and previous vulnerabilities point to poor input validation. In addition, the device does not provide for secure storage of essential security parameters.

Overall, although the RE190 adheres to several basic security principles, it falls short in areas crucial to full compliance, especially those linked to secure communication, software integrity, and protection against exploitation.

Critical reflection

A recurring trade-off in consumer IoT is revealed by the study of the TP-Link RE190 AC750: strong security is frequently sacrificed for price. The device satisfies a number of ETSI EN 303 645 requirements, including manual updates and enforced password setup, however it is devoid of crucial safeguards like firmware integrity checks and secured local access.

These discrepancies are a reflection of larger issues in the creation of IoT products, where security is often neglected. Manufacturers must embrace secure-by-design concepts and view baseline requirements as necessary rather than optional in order to guarantee long-term trust and resilience.

Conclusion

The TP-Link RE190 AC750 satisfies a number of ETSI EN 303 645 fundamental standards, such as vulnerability reporting, manual upgrades, and secure configuration. It is lacking, nonetheless, in crucial areas including input validation, firmware integrity, and encrypted communication. Although it is appropriate for daily usage, it is devoid of the safeguards required for complete compliance. Future updates would improve its overall cybersecurity by filling in these gaps.

References and Sources

TP-Link Official Product Page – TP-Link RE190 AC750
https://www.tp-link.com/en/home-networking/range-extender/re190/

TP-Link RE190 User Guide (PDF)
https://www.tp-link.com/us/support/download/re190/v3/#manual

TP-Link Quick Installation Guide – RE190
https://static.tp-link.com/2021/202112/20211223/7106509659_QIG_RE190(EU)_V3.pdf

TP-Link Security Advisory Portal (Vulnerability Disclosure Policy)
https://www.tp-link.com/en/security/

TP-Link Privacy Policy
https://www.tp-link.com/en/about-us/privacy-policy/

TP-Link Terms of Use
https://www.tp-link.com/en/about-us/terms-of-use/

CVE-2019-7406 – Remote Code Execution in TP-Link RE series devices
https://nvd.nist.gov/vuln/detail/CVE-2019-7406

SecurityWeek Article on TP-Link Input Validation Vulnerability
https://www.securityweek.com/vulnerability-exposes-tp-link-wi-fi-extenders-remote-hacking/

Firmware Update Instructions (from User Guide)
https://static.tp-link.com/2021/202112/20211223/7106509659_QIG_RE190(EU)_V3.pdf (p. 8–9)

TP-Link Community Forums – Discussion of WPA2 “Weak Security” Fix
https://community.tp-link.com/en/home/forum/topic/208370

Public technical analyses of TP-Link extender firmware
https://www.exploit-db.com/docs/english/49922-tp-link-wifi-extenders-firmware-analysis.pdf