Firmware-Inventur

Musterbericht mit Build-Unterlagen · Tasmota 16.0.0 für ESP32

Prüfgegenstand	`tasmota32.bin` aus dem Release v16.0.0
SHA-256	`977fd69e58cbae01b8298dade7e7a30eefa5ac5c58b06e021ee63618bfc9add6`
Unterlagen	Linker-Map des Releases, Quellstand v16.0.0, Framework-Paket v3.3.12, `sdkconfig.h`
Schwachstellendaten	NVD, CISA KEV, GitHub-Hinweise von Espressif, Hinweise von mbed TLS, abgefragt am 08.11.2026
Erstellt von	steitec, hello@steitec.net
Fassung	1.0 vom 08.11.2026

> Dies ist ein Beispiel auf Grundlage einer frei verfügbaren Firmware. Es zeigt, was mit Build-Unterlagen möglich ist. Aussagen gelten nur für dieses Build; andere Tasmota-Varianten haben andere Funktionen. Der Bericht ist keine Rechtsberatung und keine Bestätigung einer Konformität mit dem Cyber Resilience Act.

1. Ergebnis

140	134	26	0	1
gelinkte Bibliotheken	mit Version	Hinweise bewertet	davon nachweislich betroffen	offen

Bewertung (26 Hinweise)	Anzahl
Betroffen	**0**
Offen	1
Code teilweise vorhanden, Funktion im Build nicht aktiv	15
Nicht betroffen	10

Das Ergebnis heißt nicht, dass die Firmware sicher ist. Für viele Bestandteile gibt es keine verwertbaren Daten (Abschnitt 6).

Empfehlungen

1. **Nicht auf eine CVE-Suche allein verlassen.** Für ESP-IDF, lwIP und FreeRTOS lieferte die NVD keinen einzigen Treffer. Relevante Hinweise stehen bei Espressif und mbed TLS, sie müssen dort laufend verfolgt werden.
2. **Funktionsänderungen neu bewerten.** Die Bluetooth-Treffer sind nur entschärft, solange `USE_BLE_ESP32` aus bleibt. Ein Build mit Bluetooth braucht eine eigene Bewertung.
3. **Eigene Forks dokumentieren.** BearSSL, PubSubClient und WireGuard liegen als angepasste Kopien im Quellbaum. Ihre Herkunft und ihr Stand sollten festgehalten werden.

2. Vorgehen

1. Firmware mit der Release-Datei auf GitHub abgeglichen (gleicher SHA-256); Flash-Modus DIO aus dem Image-Kopf gelesen, passend zur verwendeten `sdkconfig.h`
2. Alle gelinkten Bibliotheken aus der Linker-Map gelesen
3. Versionen aus Bibliotheksdaten, Headern des Frameworks und `versions.txt` bestimmt
4. Plattformstand über `platformio_tasmota32.ini` nachverfolgt: Plattform 2026.09.50, Arduino 3.3.12, ESP-IDF 5.5.5

5. Abweichung des Tasmota-Forks von ESP-IDF 5.5.5 geprüft: ein Commit mit Anpassungen, keine Änderungen an lwIP, Bluetooth oder mbed TLS
6. NVD und CISA KEV abgefragt; alle GitHub-Hinweise von Espressif zu ESP-IDF und mDNS ausgewertet
7. Treffer gegen `sdkconfig.h`, die Linker-Map und die Build-Konfiguration von Tasmota geprüft

Die Firmware wurde nicht ausgeführt.

3. Zentrale Komponenten

Komponente	Version	Nachweis	Vertrauen
ESP-IDF (Tasmota-Fork)	5.5.5	Image-Kopf, `versions.txt`	hoch
Arduino-Core	3.3.12	Paketdaten, Binärdatei	hoch
mbed TLS	3.6.6	Header `build_info.h`	hoch
lwIP	2.2.0	Header `init.h`	hoch
FreeRTOS-Kernel	V10.5.1	Header `task.h`	hoch
mDNS	1.13.1	`versions.txt`	hoch
LittleFS	1.22.3	`versions.txt`	hoch
BearSSL (Fork)	0.6 laut Bibliotheksdaten	Quellstand	mittel
Berry (Fork)	7.0 laut Bibliotheksdaten	Quellstand	mittel
Wi-Fi- und Bluetooth-Bibliotheken von Espressif	Stand ESP-IDF 5.5.5	Linker-Map, nur Binärform	niedrig

Die Stückliste liegt vollständig in `sbom.cdx.json` vor (CycloneDX 1.6, gegen das offizielle Schema validiert).

Vergleich mit dem Test ohne Unterlagen: Ein Binärscanner fand in derselben Firmware keine einzige Komponente. Mit der Linker-Map sind alle 140 Bibliotheken benannt, 134 davon mit Version.

4. Bewertung

Offen

Hinweis	Komponente	CVSS	Offene Frage
CVE-2026-3285	Berry	3,3	Betrifft `scan_string`, laut NVD bis Version 1.1.0, Zugriff nur lokal. Die Funktion ist im Tasmota-Fork vorhanden; ob der Fix enthalten ist, wurde nicht geprüft

Code teilweise vorhanden, Funktion im Build nicht aktiv

Teile von NimBLE sind gelinkt. `USE_BLE_ESP32` ist in der Konfiguration von `tasmota32` aber auskommentiert, Bluetooth wird in diesem Build demnach nicht gestartet. Die Treffer stammen aus einer Suche über alle NimBLE-Versionen, die Version in ESP-IDF wurde nicht ermittelt.

Hinweise	Komponente	Anzahl
CVE-2026-45813, CVE-2025-62235, CVE-2024-24746, CVE-2024-51569, CVE-2025-52435	NimBLE	5
CVE-2025-53477, CVE-2026-45811, CVE-2026-45815, CVE-2026-45816, CVE-2026-45812	NimBLE	5
CVE-2024-47248, CVE-2026-46452, CVE-2024-47249, CVE-2024-47250, CVE-2025-53470	NimBLE	5

Nicht betroffen

Hinweis	Komponente	CVSS	Begründung
CVE-2026-113780	ESP-IDF	kritisch	ESP-TEE ist im Build nicht enthalten

Hinweis	Komponente	CVSS	Begründung
CVE-2026-113783	lwIP in ESP-IDF	hoch	Setzt `CONFIG_LWIP_DNS_MAX_HOST_IP` größer 1 voraus; hier 1
CVE-2026-113781	ESP-IDF	hoch	BLE Mesh ist nicht gelinkt
CVE-2026-81508	ESP-IDF	mittel	Betrifft Bluedroid; das Build nutzt NimBLE
CVE-2026-64860	mDNS	mittel	Betrifft Versionen vor 1.11.2; hier 1.13.1
CVE-2026-16554	cJSON	7,8	`libjson` ist nicht gelinkt
CVE-2026-67215	cJSON	7,5	wie oben
CVE-2026-67216	cJSON	5,9	wie oben
CVE-2026-67217	cJSON	5,3	wie oben
CVE-2025-66442	mbed TLS	5,1	Von `libmbedcrypto` sind nur `sha256` und `platform_util` gelinkt; `libmbedtls` und `libmbedx509` fehlen

Weitere 20 Hinweise von mbed TLS aus dem Juli 2026 (behoben in 3.6.7) betreffen laut ihren Titeln TLS, X.509, PKCS7, RSA, ECC, DTLS oder ChaCha20. Diese Teile sind im Image nicht gelinkt. Sie sind nicht in den 26 mitgezählt und wurden nur nach Titel bewertet.

5. Stückliste und BSI TR-03183-2

Abgleich mit den Pflichtfeldern der Fassung 2.1.0. Der Bericht bescheinigt keine Konformität.

Pflichtfeld	Stand	Anmerkung
Ersteller der SBOM, Zeitstempel	erfüllt	
Format CycloneDX mindestens 1.6	erfüllt	Schema validiert
Name, Version	teilweise	6 Bibliotheken ohne Version, darunter Teile der Toolchain
Abhängigkeiten	teilweise	Nur eine Ebene, als unvollständig gekennzeichnet
Dateiname, Eigenschaften	erfüllt	Bezogen auf das gelinkte Archiv
SHA-512	teilweise	67 von 140, nur vorgebaute Bibliotheken
Lizenzen	nicht erfüllt	Noch nicht erhoben
Komponentenersteller	nicht erfüllt	Noch nicht erhoben

6. Lücken und Grenzen

- **Fehlende Daten:** Für lwIP, FreeRTOS, BearSSL, PubSubClient, IRremoteESP8266, RadioLib und Tasmota selbst ergab die NVD keine Treffer. Das ist kein Nachweis von Sicherheit, denn die Abdeckung ist hier gering.
- **Forks:** Angepasste Bibliotheken lassen sich nicht zuverlässig einer Upstream-Version zuordnen.
- **Binär-Blobs:** 10 Bibliotheken von Espressif liegen nur in Binärform vor (Wi-Fi, Bluetooth-Controller, PHY). Ihr Inhalt wurde nicht geprüft.
- **LTO:** Tasmota-Bibliotheken werden mit Link-Time-Optimierung gebaut. Die Map zeigt für sie, dass sie eingebunden sind, aber nicht, welcher Code tatsächlich übrig bleibt.
- **Kein eigener Code:** Der Tasmota-Code selbst wurde nicht auf Schwachstellen geprüft.
- **Hardware:** Sicherheitshinweise zum ESP32-Chip, etwa AR2025-004 zu Bluetooth-Befehlen, sind nicht bewertet.
- **Methode:** Statische Prüfung; Aussagen zu Bluetooth stützen sich auf die Konfiguration im Quellstand.