# Firmware-Inventur

Musterbericht · OpenWrt 23.05.6 für TP-Link Archer C7 v2

| | |
|---|---|
| **Prüfgegenstand** | `openwrt-23.05.6-ath79-generic-tplink_archer-c7-v2-squashfs-sysupgrade.bin` |
| **SHA-256** | `c2a14a43f7cde3b0b122c64ed3f8ea4e4d85eccec2d3f8d991abfc2985b3680d` (entspricht der Prüfsummenliste von OpenWrt) |
| **Schwachstellendaten** | NVD und CISA KEV, 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. Die Reihe 23.05 wurde bewusst gewählt, weil sie nicht mehr aktuell ist (aktuell: 25.12.6); Aussagen über andere OpenWrt-Versionen lassen sich daraus nicht ableiten. Der Bericht ist keine Rechtsberatung und keine Bestätigung einer Konformität mit dem Cyber Resilience Act.

## 1. Ergebnis

| 148 | 3.390 | 33 | 8 | 1 |
|---|---|---|---|---|
| Komponenten erfasst | Treffer der Versionssuche | Treffer einzeln bewertet | davon betroffen | betroffen und aktiv ausgenutzt |

Eine Suche nach Versionsnummern liefert für dieses Image 3.390 Treffer. Bewertet wurden einzeln alle 29 Treffer außerhalb des Kernels sowie alle vier aktiv ausgenutzten Kernel-Lücken.

| Bewertung (33 Treffer) | Anzahl |
|---|---|
| Betroffen oder wahrscheinlich betroffen | **8** |
| Code vorhanden, in diesem Image nicht angreifbar genutzt | 9 |
| Nicht betroffen | 16 |

Von den Kernel-Treffern wurden 1.262 belegt ausgeschlossen. **2.099 Kernel-Treffer bleiben unbewertet** (Abschnitt 6).

### Empfehlungen

1. **Auf eine gepflegte OpenWrt-Version umstellen.** CVE-2026-46300 steht auf der KEV-Liste, wird also aktiv ausgenutzt, und ist erst ab Kernel 5.15.208 behoben. Das Image nutzt 5.15.189.
2. **mbed TLS 2.28 ablösen.** Der Hersteller gibt für diesen Zweig keine Korrekturen mehr heraus. Konkret liest die Bibliothek ihre Zufallsdaten hier aus `/dev/urandom` (CVE-2026-34871).
3. **Die offenen Kernel-Treffer gegen die neue Version nachprüfen**, statt sie für die alte Version einzeln abzuarbeiten.

## 2. Vorgehen

Die Firmware wurde nicht ausgeführt.

1. Image zerlegt in Kernel-Abbild (LZMA ab Offset `0x200`) und SquashFS-Dateisystem (ab Offset `2344012`)
2. Inventar aus der Paketdatenbank `opkg`; Versionen stichprobenartig gegen Texte in den Binärdateien geprüft
3. Dateien außerhalb der Paketdatenbank gesucht, insbesondere Binär-Blobs
4. 14 Hauptkomponenten in der NVD abgefragt, dazu Abgleich mit CISA KEV

5. Treffer gegen das Image geprüft: importierte Funktionen aller 87 Programme und Bibliotheken, Compile-Optionen, Plattform, Applets
6. Kernel gegen die Symboltabelle des veröffentlichten Debug-Kernels sowie die 72 Module im Image geprüft
7. Patch-Listen im Tag `v23.05.6` und Sicherheitshinweise von mbed TLS ausgewertet

## 3. Zentrale Komponenten

| Komponente | Version | Nachweis | Vertrauen |
|---|---|---|---|
| Linux-Kernel | 5.15.189 | Paketdatenbank, Versionstext | hoch |
| dropbear (SSH) | 2022.82-6 | Paketdatenbank, Binärdatei | hoch |
| dnsmasq (DNS/DHCP) | 2.90-2 | Paketdatenbank, Binärdatei | hoch |
| BusyBox | 1.36.1-1 | Paketdatenbank, Binärdatei | hoch |
| musl libc | 1.2.4-4 | Paketdatenbank, Binärdatei | hoch |
| ppp | 2.4.9 (Git-Stand) | Paketdatenbank, Binärdatei | hoch |
| nftables | 1.0.8-1 | Paketdatenbank, Binärdatei | hoch |
| mbed TLS | 2.28.10-1 | Paketdatenbank, Dateiname | mittel |
| hostapd/wpad | Git-Stand 2023-09-08 | Paketdatenbank; Binärdatei meldet `v2.11-devel` | mittel |

Vollständig: `sbom.cdx.json` mit allen 148 Einträgen (CycloneDX 1.6, gegen das offizielle Schema validiert).

## 4. Bewertung der Treffer

### Betroffen oder wahrscheinlich betroffen

| CVE | Komponente | CVSS | Begründung | Priorität |
|---|---|---|---|---|
| **CVE-2026-46300** (KEV) | Kernel | 7,8 | `skb_try_coalesce` enthalten, Korrektur erst ab 5.15.208 | **hoch** |
| CVE-2026-34871 | mbed TLS | 6,7 | Importiert weder `getrandom` noch `syscall`, liest `/dev/urandom` per `fopen`; `wpad` nutzt diese Quelle. Riskant vor allem kurz nach dem Start | mittel |
| CVE-2026-12969 | dnsmasq | 5,3 | Version im betroffenen Bereich, kein passender Patch in der Liste; Quellcode nicht geprüft | mittel |
| CVE-2023-42363 | BusyBox | 5,5 | Applet `awk` vorhanden, kein Patch; setzt präpariertes awk-Programm auf dem Gerät voraus | niedrig |
| CVE-2023-42364 | BusyBox | 5,5 | wie oben | niedrig |
| CVE-2023-42365 | BusyBox | 5,5 | wie oben | niedrig |
| CVE-2023-42366 | BusyBox | 5,5 | wie oben | niedrig |
| CVE-2025-46394 | BusyBox | 3,2 | Applet `tar` vorhanden; nur irreführende Anzeige | niedrig |

### Code vorhanden, in diesem Image nicht angreifbar genutzt

Grundlage sind die importierten Funktionen. Aufrufe innerhalb einer Bibliothek sind damit nicht erfasst.

| CVE | Komponente | CVSS | Begründung |
|---|---|---|---|
| CVE-2026-34877 | mbed TLS | 9,8 | Kein Programm ruft die Serialisierung auf (`mbedtls_ssl_context_load`, `_session_load`) |
| CVE-2025-47917 | mbed TLS | 8,9 | Kein Programm ruft `mbedtls_x509_string_to_names` auf |
| CVE-2025-26519 | musl | 8,1 | Kein Programm importiert `iconv` |

| CVE | Komponente | CVSS | Begründung |
|---|---|---|---|
| CVE-2023-52353 | mbed TLS | 7,5 | Kein Programm ruft `mbedtls_ssl_session_reset` auf |
| CVE-2021-43666 | mbed TLS | 7,5 | Kein Programm ruft `mbedtls_pkcs12_derivation` auf |
| CVE-2026-58374 | hostapd | 6,5 | Wi-Fi-7-Funktion; die Funkhardware (ath9k, ath10k) kann kein 802.11be |
| CVE-2025-52497 | mbed TLS | 4,8 | Setzt nicht vertrauenswürdige, verschlüsselte PEM-Daten voraus; eingelesen werden lokale Schlüsseldateien |
| CVE-2025-48965 | mbed TLS | 4,0 | Nur beim Erzeugen von Zertifikaten aus nicht vertrauenswürdigen Eingaben; `px5g` erhält lokale Angaben |
| CVE-2025-24912 | hostapd | 3,7 | Nur mit eingerichtetem RADIUS-Server; im Feld zu prüfen |

### Nicht betroffen

| CVE | Komponente | CVSS | Begründung |
|---|---|---|---|
| CVE-2022-48174 | BusyBox | 9,8 | Laut Beschreibung nur vor 1.35; vermutlich falsche Zuordnung in der Datenbank |
| CVE-2026-34872 | mbed TLS | 9,1 | Laut Beschreibung nur 3.5.x/3.6.x und TF-PSA-Crypto |
| CVE-2026-53266 (KEV) | Kernel | 8,8 | `CONFIG_BRIDGE_EBT_SNAT` nicht gesetzt, kein ebtables-Modul |
| CVE-2025-39964 (KEV) | Kernel | 7,8 | `AF_ALG` nicht gebaut, kein Modul |
| CVE-2026-31431 (KEV) | Kernel | 7,8 | wie oben |
| CVE-2025-52496 | mbed TLS | 7,8 | AES-NI gibt es nur auf x86; das Gerät ist MIPS |
| CVE-2026-25835 | mbed TLS | 7,7 | Kein Programm nutzt PSA-Funktionen, kein TLS 1.3; kein Klonen laufender Systeme |
| CVE-2021-45451 | mbed TLS | 7,5 | `psa_aead_generate_nonce` ist in der Bibliothek nicht enthalten |
| CVE-2025-54764 | mbed TLS | 6,2 | Laut Hinweis nur bestimmte Arm-v9-CPUs oder TrustZone-M |
| CVE-2025-60876 | BusyBox | 6,5 | Applet `wget` nicht gebaut; `/usr/bin/wget` zeigt auf `uclient-fetch` |
| CVE-2022-37660 | hostapd | 6,5 | PKEX nicht in `wpad` enthalten |
| CVE-2023-48795 | dropbear | 5,9 | Patch `021-Implement-Strict-KEX-mode`, Kennung `kex-strict-*` in der Binärdatei |
| CVE-2026-12725 | dnsmasq | 5,9 | Binärdatei meldet `no-DNSSEC`, Voraussetzung fehlt |
| CVE-2025-59438 | mbed TLS | 5,3 | PSA ungenutzt; laut Hinweis ist die Bibliothek über die Legacy-API nicht verwundbar |
| CVE-2025-66442 | mbed TLS | 5,1 | Nur mit LLVM-Optimierung; das Image ist mit GCC 12.3 gebaut |
| CVE-2022-4603 | ppp | 4,3 | Werkzeug `pppdump` nicht im Image |

## 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 | erfüllt | Blobs: Dateidatum als Version, wie von der TR vorgesehen |
| Abhängigkeiten | teilweise | Aus Paketdaten, als unvollständig gekennzeichnet |

| Pflichtfeld | Stand | Anmerkung |
|---|---|---|
| Dateiname, Eigenschaften, SHA-512 | teilweise | 9 Metapakete ohne eigene Datei; sonst Hash nur über die größte Datei je Paket |
| Lizenzen | teilweise | 139 von 146 Paketen als SPDX; 4 Freitext, 3 ohne Angabe; Blobs ohne Angabe |
| Komponentenersteller | nicht erfüllt | Eingetragen ist OpenWrt als Paketierer; Ursprungsprojekte sind nicht ermittelt |

## 6. Lücken und Grenzen

- **Kernel:** 3.361 Treffer. Ausgeschlossen: 82 andere Architektur, 1.180 nicht gebaute Subsysteme. Von den verbleibenden 2.099 wurden nur die aktiv ausgenutzten einzeln bewertet. Die Filterung beruht auf dem Subsystem in der CVE-Beschreibung; in der Restmenge sind noch viele nicht gebaute Bestandteile.
- **mbed TLS:** Der Hersteller veröffentlichte im Juli 2026 weitere 20 Hinweise. Sie wurden nicht einzeln bewertet. Der Zweig 2.28 wird dort nicht mehr gepflegt.
- **Binär-Blobs:** `ath10k/QCA988X/hw2.0/firmware-2.bin` und `board.bin` lassen sich nicht aufschlüsseln. Version und Inhalt sind unbekannt.
- **Bootloader:** Nicht Teil des Images und nicht erfasst.
- **Nicht abgefragte Komponenten:** OpenWrt-eigene Projekte wie `ubus`, `procd`, `netifd`, `uhttpd` und `odhcpd` haben in den Paketdaten keine CPE-Kennung und sind nicht ausgewertet. Für json-c, libmnl, libnftnl, iw, jansson und nftables ergab die Abfrage keine Treffer.
- **Methode:** Nur statische Prüfung, keine Tests im Betrieb. Datenbanken können fehlen oder irren; ein Beispiel ist CVE-2022-48174. Der Nachweis „nicht genutzt“ deckt keine Aufrufe innerhalb von Bibliotheken ab.