Firmware-Inventur

Musterbericht bei vorhandener Stückliste · Yocto 5.0.21 LTS für BeagleBone

Prüfgegenstand	`core-image-sato-beaglebone-yocto.rootfs.tar.bz2`, `zImage`, U-Boot und MLO aus Yocto 5.0.21
SHA-256 Rootfs	`6ea34de7fc76cfe1c0f5ea08fbcbeb38446e2d9fecec7a0c9b5e006f518e9f6b` (alle Artefakte gegen die Prüfsummen des Projekts bestätigt)
Unterlagen	Mitgelieferte SPDX-Stückliste und Paketliste, Kernel-Konfiguration aus dem Image, Quellstand `yocto-5.0.21`
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 eines frei verfügbaren Referenz-Builds. Das Yocto-Projekt veröffentlicht solche Images zum Testen, nicht als fertiges Produkt. Der Befund zeigt ein Risiko, das auch in eigenen Builds auftreten kann. Der Bericht ist keine Rechtsberatung und keine Bestätigung einer Konformität mit dem Cyber Resilience Act.

1. Ergebnis

1.054	5.808	63	17	8
Pakete aus 245 Rezepten	Treffer der Versionssuche	einzeln bewertet	davon betroffen	aktiv ausgenutzt und betroffen

Hauptbefund: Die CVE-Angaben zum Kernel stimmen für dieses Image nicht

Die mitgelieferte Stückliste führt für den Kernel 14.182 CVEs als behoben. Diese Liste wurde für **Kernel 6.6.151** erzeugt. Für das BeagleBone ist der Kernel aber auf **6.6.21** festgelegt, und das Kernel-Abbild meldet genau diese Version.

Von den 5.488 Kernel-Treffern der NVD sind **4.863 in der Yocto-Liste als behoben geführt, obwohl die Korrektur erst nach 6.6.21 kam.** Wer der Stückliste vertraut, übersieht sie. Darunter sind alle zwölf aktiv ausgenutzten Kernel-Lücken, von denen acht dieses Image betreffen. Yocto kennt das Problem und gibt beim CVE-Check eine Warnung aus; in der fertigen Stückliste ist davon nichts mehr zu sehen.

Bewertung (63 Treffer)	Anzahl
Betroffen	**17**
Offen	6
Code vorhanden, in diesem Image nicht angreifbar genutzt	11
Nicht betroffen	29

Empfehlungen

1. **Kernel aktualisieren.** Mit dem aktuellen Stand der Reihe 6.6 entfallen die acht aktiv ausgenutzten Lücken, die dieses Image betreffen.
2. **Die CVE-Angaben zur tatsächlichen Kernel-Version erzeugen.** Weicht `LINUX_VERSION` von der Version der Ausschlussliste ab, darf der Status nicht übernommen werden.
3. **Nicht Benötigtes entfernen.** Ein Produkt braucht weder 181 GStreamer-Module noch eine Demo-Oberfläche. Das senkt die Trefferzahl stärker als jede Bewertung.

4. **expat und OpenSSL nachziehen**, die von Yocto für ihre Version nicht als behoben geführten Punkte sind im Abschnitt 4 genannt.

2. Vorgehen

1. Prüfsummen aller Artefakte bestätigt; Rootfs entpackt, Kernel-Abbild dekomprimiert
2. Kernel-Version aus dem Abbild gelesen, Konfiguration aus `IKCONFIG` extrahiert
3. SPDX-Stückliste ausgewertet: Rezepte, Paketzuordnung, CPE-Kennungen und „CVEs fixed“
4. Herkunft der Kernel-Angaben im Quellstand nachvollzogen (`cve-exclusion_6.6.inc`, BSP-Rezept)
5. 237 Rezepte mit CPE-Kennung in der NVD abgefragt, Abgleich mit CISA KEV
6. Kernel-Treffer nach Subsystem gegen die echte Konfiguration gefiltert
7. Ausgewählte Treffer gegen das Image geprüft: importierte Funktionen, installierte Programme, Konfigurationsdateien

Die Firmware wurde nicht ausgeführt.

3. Zentrale Komponenten

Komponente	Version	Nachweis	Vertrauen
Linux-Kernel	6.6.21	Versionstext im Abbild, SPDX	hoch
U-Boot, SPL	2024.01	Text im Abbild	hoch
glibc	2.39 (Git-Stand)	SPDX	mittel
OpenSSL	3.5.8	SPDX, Paketliste	hoch
dropbear (SSH)	2022.83	SPDX; `ssh` und `scp` verweisen auf dropbear	hoch
OpenSSH	9.6p1, nur `sftp-server`	Paketliste, Dateifund	hoch
Avahi	0.8	SPDX	hoch
expat	2.8.3	SPDX	hoch
BlueZ, ConnMan, wpa_supplicant	5.72, 1.42, 2.10	SPDX	hoch

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

4. Bewertung der Treffer

Aktiv ausgenutzte Kernel-Lücken (alle in Yocto als behoben geführt)

CVE	CVSS	Korrektur ab	Bewertung	Begründung
CVE-2024-36971	7,8	6.6.34	**betroffen**	Netzwerk-Kern
CVE-2024-50302	5,5	6.6.61	**betroffen**	`CONFIG_HID=y`; Angriff über USB-Gerät
CVE-2025-38352	7,8	6.6.94	**betroffen**	POSIX-Timer, auf ARM32 der betroffene Pfad
CVE-2025-39964	7,8	6.6.108	**betroffen**	Modul `af_alg` im Image
CVE-2026-31431	7,8	6.6.137	**betroffen**	Modul `algif_aead` im Image
CVE-2026-46300	7,8	6.6.141	**betroffen**	Netzwerk-Kern
CVE-2026-53266	8,8	6.6.143	**betroffen**	Modul `ebt_snat` im Image, `CONFIG_USER_NS=y`
CVE-2026-53362	7,8	6.6.144	**betroffen**	`CONFIG_IPV6=y`
CVE-2025-39682	9,8	6.6.103	nicht betroffen	`CONFIG_TLS` nicht gesetzt
CVE-2024-53104	7,8	6.6.61	nicht betroffen	`uvcvideo` nicht gebaut

CVE	CVSS	Korrektur ab	Bewertung	Begründung
CVE-2024-53150	7,1	6.6.64	nicht betroffen	`snd-usb-audio` nicht gebaut
CVE-2024-53197	7,8	6.6.64	nicht betroffen	wie oben

Weitere betroffene Komponenten

Hinweise	Komponente	Einschätzung
CVE-2026-66046, CVE-2026-115506, CVE-2026-76956, CVE-2026-113351, CVE-2026-117610, CVE-2026-118370, CVE-2026-76957	expat 2.8.3	Version im betroffenen Bereich, kein Eintrag bei Yocto; relevant, wenn nicht vertrauenswürdiges XML verarbeitet wird
CVE-2026-35189	OpenSSL	Speicherverbrauch bei präparierten Zertifikaten; niedrig
CVE-2025-59529	Avahi	Dienst läuft im Image; lokale Clients können ihn stören

Offen

Sechs Hinweise zu glibc: CVE-2026-5450, CVE-2026-0861, CVE-2025-15281, CVE-2026-5928, CVE-2026-4437 und CVE-2026-4438. Yocto baut einen Git-Stand der Reihe 2.39. Ob die Korrektur darin enthalten ist und ob ein Programm die Funktion passend aufruft, wurde nicht geklärt.

Code vorhanden, in diesem Image nicht angreifbar genutzt

Hinweise	Anzahl	Begründung
OpenSSL QUIC: CVE-2026-54873, -84784, -42772, -75804, -35191	5	Nur das Kommandozeilenwerkzeug `openssl` importiert QUIC
OpenSSL DTLS: CVE-2026-84782, -75806	2	Nur `openssl` und das GStreamer-Modul `dtls`
OpenSSL: CVE-2026-72897, -75805, -54872, -77696	4	Kein Dienst im Image nutzt diese Pfade (Kontextwechsel, CMP, Signaturen)

Nicht betroffen (ohne Kernel)

Hinweise	Anzahl	Begründung
OpenSSH, alle 13 Treffer	13	Installiert ist nur `sftp-server`; `sshd`, `ssh`, `sftp`, `ssh-agent` und `ssh-keygen` von OpenSSH fehlen
glibc: CVE-2024-33599, -33600, -33601, -33602	4	`nscd` nicht installiert
glibc: CVE-2024-2961, CVE-2026-4046	2	Betroffene iconv-Module nicht installiert
glibc: CVE-2026-0915	1	`networks` nutzt nur `files`
glibc: CVE-2025-5702	1	Nur Power10
glibc: CVE-2013-4412	1	Falsche Zuordnung, betrifft ein anderes Programm
OpenSSL: CVE-2019-0190	1	Falsche Zuordnung, betrifft `mod_ssl`
OpenSSL: CVE-2026-54875	1	Nur ARM64 und RISC-V
Avahi: CVE-2021-26720	1	Debian-Skript im Image nicht vorhanden

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	Auf Ebene der Rezepte
Abhängigkeiten	teilweise	Nur eine Ebene, als unvollständig gekennzeichnet
Dateiname, Eigenschaften, SHA-512	teilweise	Nur für Kernel, U-Boot und SPL
Lizenzen	teilweise	Aus Yocto übernommen, nicht auf SPDX-Kennungen geprüft
Komponentenersteller	teilweise	Projektseite aus den Rezeptdaten, sonst Yocto

6. Lücken und Grenzen

- **Kernel:** Von 5.488 Treffern sind 1.333 ausgeschlossen (189 andere Architektur, 1.144 Subsystem nicht gebaut). 4.155 bleiben, von denen nur die aktiv ausgenutzten einzeln bewertet sind.
- **Weitere Komponenten:** 131 von Yocto nicht als behoben geführte Treffer sind nicht einzeln bewertet, darunter GStreamer (53), curl (19), sqlite3 (12) und X-Server (12). Einige sind falsche Zuordnungen, etwa `puzzles` zu einem WordPress-Theme.
- **Yocto-Angaben außerhalb des Kernels:** 138 als behoben geführte Treffer wurden übernommen und nicht nachgeprüft.
- **Bootloader:** U-Boot 2024.01 erfasst, 11 NVD-Treffer aber nicht bewertet. Er ist nicht Teil der SPDX-Stückliste des Images.
- **Nicht gesucht:** Dateien außerhalb der Yocto-Pakete und Binär-Blobs wurden nicht gesondert untersucht.
- **Methode:** Nur statische Prüfung. Die Kernel-Filterung beruht auf dem Subsystem in der CVE-Beschreibung.