

Firmware security assessment

OpenWrt 23.05.5 armsr-armv8 rootfs · v23.05.5

Vendor	OpenWrt
SHA-256	00bd253bfce5ea2d87c430dbbdc21528757b059d5b67b57b8f31397ddc7abbb
File size	4.0 MB
Report generated	2026-10-10 06:58 UTC
Compliance frameworks included	2

F

10.0 / 10

Overall risk score · 33/52 technical checks passed (distinct checks across frameworks) (63.5%); 4 not assessed

Scores on assessed controls · coverage shown below

ETSI EN 303 645		64.0%
41/45 mapped checks assessed		
OWASP Firmware Security Testing Methodology		68.7%
46/47 mapped checks assessed		

Automated analysis evidence supports review. Runtime coverage is limited to successfully executed targets. Organisational requirements (ETSI 5.2, EU CRA Annex I Part II) require separate manual assessment. Bars follow the A-F thresholds: green from 90%, blue from 70%, amber from 50%, rose below.

OpenWrt 23.05.5 armsr-armv8 rootfs

Vendor OpenWrt Version 23.05.5 Generated 2026-10-10 06:58 UTC File size 4.0 MB

SHA-256 00bd253bfce5ea2d87c430dbbdc21528757b059d5b67b57b8f31397ddc7abbb

Security-test grade **F** · Overall risk **10.0 / 10** · 33/52 technical checks passed (distinct checks across frameworks), 63.5% pass rate · security test suite 19/37 assessed passed, grade F

191	14	197	33
ELF/PE binaries	Critical findings	High findings	SBOM components

Assessment scope and limitations

Analysis status: **complete**.

This report presents the recorded assessment evidence. Unsupported, failed, and unassessed checks do not establish that a product is safe or compliant. Runtime observations apply only to the inputs and paths exercised.

Checks with no assessment: 4. Not applicable: 1.

Findings shown: 50 of 451. The findings export provides the detailed inventory. Assessment generated at 2026-10-10 06:58 UTC.

Executive Summary

OpenWrt 23.05.5 armsr-armv8 rootfs scored **10.0/10** risk (security-test grade **F**) with **14** critical and **197** high-severity findings. Assessed across 2 compliance frameworks. Threat model assessment found **8** applicable threats across **4** recorded-present system properties.

Top recommended actions

1. **CVE-2026-72842: openwrt 23.05.5** (2 binaries: banner, openwrt_release)

Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: <https://nvd.nist.gov/vuln/detail/CVE-2026-72842> Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.

2. **Updates install without signature verification**

Fix: Ship the updater's signing keys and enable signature verification in its configuration.

3. **CVE-2026-55159: dnsmasq 2.90** (dnsmasq)

Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: <https://nvd.nist.gov/vuln/detail/CVE-2026-55159> Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.

4. **CVE-2026-72840: busybox 1.36.1** (busybox)

Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: <https://nvd.nist.gov/vuln/detail/CVE-2026-72840> Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.

5. **UART debug shell on ttyS0**

Fix: Disable UART shell in etc/inittab. Comment out or remove the line spawning a shell on ttyS0. If UART is needed for diagnostics, require authentication before shell access. Reference: ETSI EN 303 645 Provision 5.6 - minimise exposed attack surfaces.

Runtime observations

Run completed at 2026-10-10 06:55 UTC. These are observations from this recorded run; a completed run does not mean every target executed.

Recorded targets	Targets that ran	Libraries observed	Runtime findings
206	46	27	2

Target counts may include libraries. These counts do not measure instruction or path coverage. Executing a target or observing a component does not establish CVE exploitability, and an unobserved component is not proven absent.

Compliance Framework Scores

Framework and assessed coverage	Score	Grade	Pass	Fail
ETSI EN 303 645 41/45 mapped checks assessed	64.04494382022472%	D	25	16
OWASP Firmware Security Testing Methodology 46/47 mapped checks assessed	68.70748299319727%	C	29	17

Compliance check inventory (57 checks)

ID	Test case	Severity	Result
TC-ATK-01	Telnet service detection OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.6-1, 5.6-5 · NIST IR 8259A - Capability 4 · IEC 62443-4-2 - CR 2.1 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (29.1) · CWE-319	Critical	Pass
TC-ATK-02	FTP service detection OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.6-1, 5.6-5 · IEC 62443-4-2 - CR 2.1 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (29.1) · CWE-319	High	Pass
TC-ATK-03	Debug tool presence OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.6-6 · IEC 62443-4-2 - CR 2.1 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28.2) · CWE-489 1. Remove debug tooling (gdbserver, strace, tcpdump, netcat, compilers) from production images. 2. Move these tools to a separate development/debug image variant that is never shipped to customers. 3. Add a build-time manifest check that fails if any debug tool package is present in the production image. Yocto: Split `IMAGE_INSTALL` between a `*-dev` image (with `tools-debug`, `dev-pkgs` `IMAGE_FEATURES`) and the production image; ensure production images don't include `IMAGE_FEATURES += "tools-debug debug-tweaks"`.	High	Fail
TC-ATK-04	UART debug shell detection OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.6-4 · IEC 62443-4-2 - CR 2.1 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28.2) · CWE-306 1. Disable the UART console/shell in production builds (remove the `getty`/shell spawn on the serial line from inittab or the systemd unit). 2. If UART access is needed for field diagnostics, gate it behind an authenticated unlock mechanism (e.g. signed challenge-response). 3. Confirm physical UART pins are not silk-screen labeled or easily accessible if the shell cannot be fully removed. Yocto: Remove the serial `getty` entry from `/etc/inittab` (sysvinit) or mask the `serial-getty@ttyS0.service` (systemd) in the image recipe for production builds; keep it only in a debug image variant.	High	Fail

TC-ATK-05	Unnecessary network services ETSI EN 303 645 - 5.6-1, 5.6-5 · NIST IR 8259A - Capability 4 · IEC 62443-4-2 - CR 2.1 · EU CRA - Annex I Part I 2(g) · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (29.1) · CWE-1327	Medium	Pass
TC-ATK-06	Web interface privilege check OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.6-7 · IEC 62443-4-2 - CR 2.1 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · CWE-250	High	Pass
TC-ATK-07	Vulnerability disclosure policy presence ETSI EN 303 645 - 5.2-1 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.3 · IEC 81001-5-1 - 6.2 · TEC 31318 - 3.2	Medium	Not assessed
TC-ATK-08	Brute-force protection on network authentication ETSI EN 303 645 - 5.1-5 · IEC 62443-4-2 - CR 1.11 · EU CRA - Annex I Part I 2(d) · NIST IR 8259A - Capability 4 · OWASP FSTM - Stage 5 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.1	High	Pass
TC-ATK-09	Pre-authentication information disclosure ETSI EN 303 645 - 5.6-2 · EU CRA - Annex I Part I 2(k) · OWASP FSTM - Stage 5 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.1, 3.6	Medium	Fail
TC-ATK-10	Redundant root-privileged account EN 18031-1 - GEC-2 · ETSI EN 303 645 - 5.6-7 · FDA 524B - (b)(2) · IEC 62443-4-2 - CR 2.1 · OWASP FSTM - Stage 5 · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6	Critical	Pass
TC-ATK-11	Security event logging present EU CRA - Annex I Part I 2(m) · IEC 62443-4-2 - CR 6.1 · NIST SP 800-193 - 4.1.4 · OWASP FSTM - Stage 5 · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.10	Medium	Pass
TC-ATK-12	Management interface served over cleartext HTTP OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5-1 · NIST IR 8259A - Capability 3 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - GEC-2 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-319	High	Fail
TC-BIN-01	Stack canary detection OWASP FSTM - Stage 5 · EN 18031-1 - GEC-1 · IEC 81001-5-1 - 5.4 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28) · CWE-121 1. Recompile the affected binaries with <code>`-fstack-protector-strong`</code> (or <code>`-fstack-protector-all`</code> for highest-risk binaries). 2. Confirm the toolchain's libc supports <code>`__stack_chk_fail`</code> and links it in. 3. Re-run the binary hardening check to confirm the canary is present in the compiled output. Yocto: Add <code>`SECURITY_CFLAGS += "-fstack-protector-strong"'</code> (or use the <code>`meta-security`</code> distro feature <code>`stack-protector`</code>) in your distro/local.conf rather than per-recipe.	Medium	Fail
TC-BIN-02	NX/DEP bit verification OWASP FSTM - Stage 5 · EN 18031-1 - GEC-1 · IEC 81001-5-1 - 5.4 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28) · CWE-119	High	Pass
TC-BIN-03	PIE/ASLR verification OWASP FSTM - Stage 5 · EN 18031-1 - GEC-1 · IEC 81001-5-1 - 5.4 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28) · CWE-121 1. Recompile critical binaries as position-independent executables (<code>`-fPIE -pie`</code>). 2. Ensure the kernel has ASLR enabled (<code>`/proc/sys/kernel/randomize_va_space = 2`</code>). 3. Re-check binary type is <code>`ET_DYN`</code> (PIE) rather than <code>`ET_EXEC`</code> . Yocto: Enable the <code>`pie`</code> security flag via <code>`SECURITY_CFLAGS`/`SECURITY_LDFLAGS`</code> (Yocto's <code>`security_flags.inc`</code>); some BSP recipes explicitly disable PIE for bootloaders/init - confirm that's intentional and documented.	Medium	Fail
TC-BIN-04	RELRO configuration OWASP FSTM - Stage 5 · EN 18031-1 - GEC-1 · IEC 81001-5-1 - 5.4 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28) · CWE-1188	Low	Pass

TC-BIN-05	Debug symbol stripping OWASP FSTM - Stage 5 · EN 18031-1 - GEC-1 · IEC 81001-5-1 - 5.4 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28.2) · CWE-215 - Strip debug sections (<code>debug_*</code>, <code>.symtab</code> where not required) from production binaries with <code>strip --strip-unneeded</code>. - Keep unstripped copies + debug symbols (<code>debug</code> packages or a symbol server) for internal crash-analysis only - never ship them. - Add a build-time check that fails the image build if any installed binary still contains debug sections. Yocto: Yocto strips by default via <code>INHIBIT_PACKAGE_STRIP = "0"</code> and <code>do_package</code> splitting <code>-dbg</code> packages - confirm <code>-dbg</code> packages aren't accidentally included in <code>IMAGE_INSTALL</code> for production images.	Low	Fail
TC-BIN-06	Insecure RPATH/RUNPATH OWASP FSTM - Stage 5 · EN 18031-1 - GEC-1 · IEC 81001-5-1 - 5.4 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.6 · UN R155 - Annex 5 Part A 4.3.7 (28) · CWE-426	Medium	Pass
TC-B00T-01	Bootloader signature verification NIST SP 800-193 - 4.1.1 · ETSI EN 303 645 - 5.7-1 · IEC 62443-4-2 - CR 3.4 · EU CRA - Annex I Part I 2(j) · EN 18031-1 - RLM-1 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.1 · TEC 31318 - 3.7 · UN R155 - Annex 5 Part A 4.3.6 (23) · CWE-347	Critical	Not assessed
TC-B00T-04	Runtime integrity verification NIST SP 800-193 - 4.2.1 · ETSI EN 303 645 - 5.7-1 · EU CRA - Annex I Part I 2(j) · EN 18031-1 - RLM-1 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.1 · TEC 31318 - 3.7 · UN R155 - Annex 5 Part A 4.3.6 (23) · CWE-354 - Compute a cryptographic hash (or signature) over critical runtime partitions/binaries at boot time. - Verify the computed hash against an expected value stored in protected storage before continuing boot. - Define and test the failure behavior (halt, recovery boot, or alert) when verification fails. Yocto: Enable dm-verity for the rootfs partition (<code>CONFIG_DM_VERITY</code> in the kernel, plus <code>IMAGE_FSTYPES</code> integration) so runtime integrity is enforced transparently by the block layer.	High	Fail
TC-B00T-05	No published test keys in Secure Boot databases NIST SP 800-193 - 4.1.1 · ETSI EN 303 645 - 5.7-1 · IEC 62443-4-2 - CR 3.4 · EU CRA - Annex I Part I 2(j) · EN 18031-1 - RLM-1 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.1 · CWE-1394 · CWE-321	Critical	Not applicable
TC-CODE-01	Command or code injection in shipped scripts ETSI EN 303 645 - 5.13-1 · IEC 62443-4-2 - CR 3.5 · OWASP FSTM - Stage 5 · EU CRA - Annex I Part I 2(b) · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.13 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	Critical	Fail
TC-CODE-02	Untrusted input rendered by the device web interface ETSI EN 303 645 - 5.13-1 · IEC 62443-4-2 - CR 3.5 · OWASP FSTM - Stage 5 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.13 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	Medium	Pass
TC-CODE-03	Untrusted input selects a file path ETSI EN 303 645 - 5.13-1 · IEC 62443-4-2 - CR 3.5 · OWASP FSTM - Stage 5 · EU CRA - Annex I Part I 2(b) · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.13 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	High	Pass
TC-CODE-04	Untrusted data parsed by an interpreter or database ETSI EN 303 645 - 5.13-1 · IEC 62443-4-2 - CR 3.5 · OWASP FSTM - Stage 5 · EU CRA - Annex I Part I 2(b) · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.13 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	High	Fail
TC-CRED-01	Hardcoded credential detection OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.1-1 · NIST IR 8259A - Capability 4 · IEC 62443-4-2 - CR 1.5 · EU CRA - Annex I Part I 2(b) · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.1 · UN R155 - Annex 5 Part A 4.3.7 (28.2) · CWE-798	Critical	Pass
TC-CRED-02	Default credential database match ETSI EN 303 645 - 5.1-1, 5.1-2 · NIST IR 8259A - Capability 2 · IEC 62443-4-2 - CR 1.1 · EU CRA - Annex I Part I 2(a) · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.1 · UN R155 - Annex 5 Part A 4.3.7 (28.2) · CWE-798 · CWE-259	Critical	Pass
TC-CRED-03	Password hash strength assessment OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.4-1 · IEC 62443-4-2 - CR 1.5 · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.4 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-916	High	Pass

TC-CRED-04	API key and token detection OWASP FSTM - Stage 5 · IEC 62443-4-2 - CR 1.5 · EU CRA - Annex I Part I 2(b) · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.4 · UN R155 - Annex 5 Part A 4.3.7 (28.2) · CWE-798	High	Pass
TC-CRED-05	Embedded private key detection OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.4-3 · IEC 62443-4-2 - CR 1.5 · EU CRA - Annex I Part I 2(b) · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.4 · UN R155 - Annex 5 Part A 4.3.6 (19.3) · CWE-321	Critical	Pass
TC-CRED-06	Credentials stored in clear text on the device ETSI EN 303 645 - 5.4-1 · EU CRA - Annex I Part I 2(c) · IEC 62443-4-2 - CR 4.1 · OWASP FSTM - Stage 5 · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.4 · UN R155 - Annex 5 Part A 4.3.6 (19)	High	Pass
TC-CRED-07	Account with no password set ETSI EN 303 645 - 5.1-1 · IEC 62443-4-2 - CR 1.5 · EU CRA - Annex I Part I 2(d) · NIST IR 8259A - Capability 4 · OWASP FSTM - Stage 5 · EN 18031-1 - AUM-1 · EN 18031-2 - SSM-1 · EN 18031-3 - RED 3.3(f) - AUM · IEC 81001-5-1 - 5.2.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.1 · UN R155 - Annex 5 Part A 4.3.7 (28.2)	Critical	Fail
TC-CRYPTO-01	MD5 usage in security context OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) - CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-327 1. Locate all uses of MD5 in security-relevant code paths (auth, integrity, signing). 2. Replace MD5 with SHA-256 or SHA-3 for any integrity/authentication purpose. 3. Where MD5 is used only for non-security checksums (e.g. cache keys), document the exception and ensure it cannot be reached by an attacker-controlled path. Yocto: Grep linked libraries for `MD5_Init`/`MD5_Update` symbols; if pulled in transitively via an old OpenSSL 1.0.x recipe, bump `PREFERRED_VERSION_openssl` to 3.x.	High	Fail
TC-CRYPTO-02	SHA-1 usage in security context OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) - CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-327	High	Pass
TC-CRYPTO-03	Deprecated cipher detection (DES/3DES/RC4) OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) - CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-327 1. Identify all uses of DES, 3DES, or RC4 and the data they protect. 2. Replace with AES-128/256-GCM or ChaCha20-Poly1305. 3. Re-key any data previously protected with the deprecated cipher. Yocto: Disable legacy ciphers at the crypto-library build level (e.g. mbedTLS `MBEDTLS_DES_C` off) so they can't be re-introduced by a dependency.	High	Fail
TC-CRYPTO-04	RSA key length validation OWASP FSTM - Stage 5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) - CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-326	High	Pass
TC-CRYPTO-05	TLS version enforcement OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · NIST IR 8259A - Capability 3 · IEC 62443-4-2 - CR 4.1 · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) - CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-326	Medium	Pass
TC-CRYPTO-06	Certificate validation OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · NIST IR 8259A - Capability 3 · IEC 62443-4-2 - CR 4.1 · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) - CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-295 1. Replace self-signed certificates used in production with certificates issued by a managed internal or public CA. 2. Add monitoring for certificate expiry with renewal well before the expiry date. 3. Ensure the TLS client enforces full chain + hostname validation (no `verify=False`/`InsecureSkipVerify` equivalents). Yocto: Audit provisioning recipes for `openssl req -x509 -days 36500` self-signed cert generation - replace with device-unique certs issued during manufacturing.	Medium	Fail

TC-CRYPTO-07	Hardcoded IV/salt detection OWASP FSTM - Stage 5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) · CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26) · CWE-330	High	Not assessed
TC-CRYPTO-08	Deprecated SSL protocol versions (SSLv2/SSLv3) OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · NIST IR 8259A - Capability 3 · IEC 62443-4-2 - CR 4.1 · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) · CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26)	Critical	Pass
TC-CRYPTO-09	Broken hash algorithm (MD4) OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) · CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26)	High	Fail
TC-CRYPTO-10	Weak or null cipher (RC2, null cipher suite) OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) · CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26)	High	Pass
TC-CRYPTO-11	ECB block-cipher mode OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.5 · IEC 62443-4-2 - CR 4.1 · EU CRA - Annex I Part I 2(d) · EN 18031-1 - CRY-1 · EN 18031-2 - SCM-1 · EN 18031-3 - RED 3.3(f) · CRY · IEC 81001-5-1 - 4.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.5 · UN R155 - Annex 5 Part A 4.3.7 (26)	High	Pass
TC-CVE-01	OS and kernel CVE scan OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.3 · NIST IR 8259A - Capability 5 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1) · CWE-1104	Critical	Pass
TC-CVE-02	BusyBox CVE scan OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.3 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1) · CWE-1104 - Identify the BusyBox version and check it against known CVEs with CVSS >= 7.0. - Upgrade to the latest BusyBox release for your branch, or apply the specific security backport. - Re-run the CVE scan to confirm the score drops below the threshold. Yocto: Bump `PREFERRED_VERSION_busybox` in your distro config; check `meta-oe`/`poky` for the latest maintained recipe revision.	High	Fail
TC-CVE-03	TLS library CVE check OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.3 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1) · CWE-1104	Critical	Pass
TC-CVE-04	SBOM generation NIST IR 8259A - Capability 6 · ETSI EN 303 645 - 5.3 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 5.2.4 · FDA 524B - (b)(3) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3	High	Pass
TC-CVE-05	Known vulnerable binary hash match OWASP FSTM - Stage 5 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.6 (22) · CWE-1104	Critical	Pass
TC-CVE-06	Firmware-wide critical CVE presence OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.3 · NIST IR 8259A - Capability 5 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1) · CWE-1104 - Review every CRITICAL-severity CVE finding in the firmware - not limited to the kernel/OS or any single component, this covers the whole image. - Prioritize by reachability: a CRITICAL CVE confirmed reachable from a real entry point needs an immediate patch or mitigation; one confirmed unreachable is lower urgency but should still be tracked. - Upgrade or patch each affected component to a version without the CVE, or apply a documented compensating control if an upgrade isn't immediately available. Yocto: Enable `cve-check.bbclass` across the whole image build, not just the kernel recipe, so every component's CVE exposure is tracked, not only the OS/kernel layer.	Critical	Fail
TC-CVE-07	CVE regression from prior firmware version OWASP FSTM - Stage 5 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1) · CWE-1104	High	Pass

TC-CVE-08	Any component has a HIGH-or-above or known-exploited CVE OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.3 · NIST IR 8259A - Capability 5 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	High	Fail
TC-CVE-09	End-of-life component in the SBOM OWASP FSTM - Stage 5 · ETSI EN 303 645 - 5.3 · NIST IR 8259A - Capability 5 · EU CRA - Annex I Part I 1 · IEC 81001-5-1 - 6.1 · FDA 524B - (b)(2) · ISO/SAE 21434 - 8.5, 8.6 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.7 (28.1) · CWE-1104	High	Pass
TC-RUN-01	Memory-safety fault under adversarial input EU CRA - Annex I Part I 2(b) · ETSI EN 303 645 - 5.13-1 · IEC 62443-4-2 - CR 3.5 · OWASP FSTM - Stage 7 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.13 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	Critical	Pass
TC-RUN-02	Sandbox network service and process execution observed ETSI EN 303 645 - 5.13-1 · IEC 62443-4-2 - CR 3.5 · OWASP FSTM - Stage 7 · FDA 524B - (b)(2) · ISO/SAE 21434 - 10.4.2 · TEC 31318 - 3.13 · UN R155 - Annex 5 Part A 4.3.7 (28.1)	High	Pass
TC-UPD-01	Update signature verification presence NIST SP 800-193 - 4.1.2 · ETSI EN 303 645 - 5.3-9, 5.3-10 · NIST IR 8259A - Capability 5 · IEC 62443-4-2 - CR 3.4 · EU CRA - Annex I Part I 3 · EN 18031-1 - SUM-1 · EN 18031-3 - RED 3.3(f) - SUM · IEC 81001-5-1 - 7.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 13.4 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.3 (11) · CWE-347 1. Implement signature verification (RSA-2048+, ECDSA P-256+, or Ed25519) for all firmware update packages. 2. Store the verification public key in immutable/read-only storage (not in the updatable partition). 3. Reject and log any update package that fails signature verification. Yocto: Adopt `meta-secure-core` / swupdate's signed-image support; configure `SWUPDATE_SIGNING` (or RAUC's `keyring.pem`) rather than rolling a custom verifier.	Critical	Fail
TC-UPD-02	Update channel encryption ETSI EN 303 645 - 5.3-2, 5.3-7 · NIST IR 8259A - Capability 5 · EU CRA - Annex I Part I 3 · EN 18031-1 - SUM-1 · EN 18031-3 - RED 3.3(f) - SUM · IEC 81001-5-1 - 7.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 13.4 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.3 (11) · CWE-319	High	Pass
TC-UPD-04	Pre-installation integrity check NIST SP 800-193 - 4.1.2 · ETSI EN 303 645 - 5.3-9 · EU CRA - Annex I Part I 3 · EN 18031-1 - SUM-1 · EN 18031-3 - RED 3.3(f) - SUM · IEC 81001-5-1 - 7.2 · FDA 524B - (b)(1) · ISO/SAE 21434 - 13.4 · TEC 31318 - 3.3 · UN R155 - Annex 5 Part A 4.3.3 (11) · CWE-494	Critical	Not assessed

Security Findings (451 total, showing top 50)

Severity	Type	Finding	Binary
Critical	CVE	CVE-2026-72842: openwrt 23.05.5 CVE-2026-72842 · CVSS 9.9 · EPSS 0.6% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-72842 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
Critical	CVE	CVE-2026-72842: openwrt 23.05.5 CVE-2026-72842 · CVSS 9.9 · EPSS 0.6% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-72842 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner

Critical	CVE	CVE-2026-66747: openwrt 23.05.5 CVE-2026-66747 · CVSS 9.8 · EPSS 0.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-66747 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
Critical	CVE	CVE-2026-30872: openwrt 23.05.5 CVE-2026-30872 · CVSS 9.8 · EPSS 1.1% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-30872 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
Critical	CVE	CVE-2026-66747: openwrt 23.05.5 CVE-2026-66747 · CVSS 9.8 · EPSS 0.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-66747 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
Critical	CVE	CVE-2026-30871: openwrt 23.05.5 CVE-2026-30871 · CVSS 9.8 · EPSS 0.7% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-30871 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
Critical	CVE	CVE-2026-30872: openwrt 23.05.5 CVE-2026-30872 · CVSS 9.8 · EPSS 1.1% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-30872 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
Critical	CVE	CVE-2026-30871: openwrt 23.05.5 CVE-2026-30871 · CVSS 9.8 · EPSS 0.7% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-30871 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release

Critical	CVE	CVE-2026-62948: openwrt 23.05.5 CVE-2026-62948 · CVSS 9.6 · EPSS 0.6% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-62948 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
Critical	CVE	CVE-2026-62948: openwrt 23.05.5 CVE-2026-62948 · CVSS 9.6 · EPSS 0.6% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-62948 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
Critical	CVE	CVE-2024-54143: openwrt 23.05.5 CVE-2024-54143 · CVSS 9.3 · EPSS 1.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2024-54143 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
Critical	CVE	CVE-2024-54143: openwrt 23.05.5 CVE-2024-54143 · CVSS 9.3 · EPSS 1.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2024-54143 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
Critical	UPDATE_MECHANISM	Updates install without signature verification Confidence: HIGH · Reachability evidence: Not recorded Fix: Ship the updater's signing keys and enable signature verification in its configuration.	firmware-wide
Critical	UPDATE_MECHANISM	Unsigned updates are accepted Confidence: HIGH · Reachability evidence: Not recorded Fix: Configure the updater to refuse unsigned updates (for example REQUIRE_IMAGE_SIGNATURE=1 or check_signature).	firmware-wide
High	CVE	CVE-2026-69096: openwrt 23.05.5 CVE-2026-69096 · CVSS 8.8 · EPSS 3.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-69096 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release

High	CVE	CVE-2026-46368: openwrt 23.05.5 CVE-2026-46368 · CVSS 8.8 · EPSS 7.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-46368 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-59260: openwrt 23.05.5 CVE-2026-59260 · CVSS 8.8 · EPSS 0.9% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-59260 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-26899: openwrt 23.05.5 CVE-2026-26899 · CVSS 8.8 · EPSS 0.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-26899 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-69096: openwrt 23.05.5 CVE-2026-69096 · CVSS 8.8 · EPSS 3.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-69096 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-55159: openwrt 23.05.5 CVE-2026-55159 · CVSS 8.8 · EPSS 0.5% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-55159 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-59260: openwrt 23.05.5 CVE-2026-59260 · CVSS 8.8 · EPSS 0.9% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-59260 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner

High	CVE	CVE-2026-55159: dnsmasq 2.90 CVE-2026-55159 · CVSS 8.8 · EPSS 0.5% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-55159 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	dnsmasq
High	CVE	CVE-2026-26899: openwrt 23.05.5 CVE-2026-26899 · CVSS 8.8 · EPSS 0.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-26899 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-46368: openwrt 23.05.5 CVE-2026-46368 · CVSS 8.8 · EPSS 7.8% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-46368 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-72840: busybox 1.36.1 CVE-2026-72840 · CVSS 8.8 · EPSS 0.4% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-72840 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	busybox
High	CVE	CVE-2026-72840: openwrt 23.05.5 CVE-2026-72840 · CVSS 8.8 · EPSS 0.4% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-72840 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-72840: openwrt 23.05.5 CVE-2026-72840 · CVSS 8.8 · EPSS 0.4% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-72840 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release

High	CVE	CVE-2026-55159: openwrt 23.05.5 CVE-2026-55159 · CVSS 8.8 · EPSS 0.5% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-55159 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-4892: dnsmasq 2.90 CVE-2026-4892 · CVSS 8.4 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-4892 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	dnsmasq
High	CVE	CVE-2026-29004: busybox 1.36.1 CVE-2026-29004 · CVSS 8.1 · EPSS 0.6% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-29004 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	busybox
High	CVE	CVE-2024-51240: openwrt 23.05.5 CVE-2024-51240 · CVSS 8.0 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2024-51240 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2024-51240: openwrt 23.05.5 CVE-2024-51240 · CVSS 8.0 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2024-51240 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2025-62525: openwrt 23.05.5 CVE-2025-62525 · CVSS 7.9 · EPSS 0.2% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2025-62525 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release

High	CVE	CVE-2025-62526: openwrt 23.05.5 CVE-2025-62526 · CVSS 7.9 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2025-62526 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2025-62525: openwrt 23.05.5 CVE-2025-62525 · CVSS 7.9 · EPSS 0.2% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2025-62525 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2025-62526: openwrt 23.05.5 CVE-2025-62526 · CVSS 7.9 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2025-62526 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-30874: openwrt 23.05.5 CVE-2026-30874 · CVSS 7.8 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-30874 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-30874: openwrt 23.05.5 CVE-2026-30874 · CVSS 7.8 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: HIGH · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-30874 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner
High	CVE	CVE-2026-69095: openwrt 23.05.5 CVE-2026-69095 · CVSS 7.5 · EPSS 0.9% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-69095 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner

High	CVE	CVE-2026-88830: busybox 1.36.1 CVE-2026-88830 · CVSS 7.5 · EPSS 0.4% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-88830 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	busybox
High	CVE	CVE-2026-6507: dnsmasq 2.90 CVE-2026-6507 · CVSS 7.5 · EPSS 0.6% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-6507 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	dnsmasq
High	CVE	CVE-2026-69095: openwrt 23.05.5 CVE-2026-69095 · CVSS 7.5 · EPSS 0.9% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-69095 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-4890: dnsmasq 2.90 CVE-2026-4890 · CVSS 7.5 · EPSS 1.1% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-4890 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	dnsmasq
High	CVE	CVE-2026-5172: dnsmasq 2.90 CVE-2026-5172 · CVSS 7.3 · EPSS 0.7% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-5172 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	dnsmasq
High	CVE	CVE-2023-30312: openwrt 23.05.5 CVE-2023-30312 · CVSS 7.3 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2023-30312 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	banner

High	CVE	CVE-2026-88832: busybox 1.36.1 CVE-2026-88832 · CVSS 7.3 · EPSS 0.1% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-88832 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	busybox
High	CVE	CVE-2023-30312: openwrt 23.05.5 CVE-2023-30312 · CVSS 7.3 · EPSS 0.3% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2023-30312 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	openwrt_release
High	CVE	CVE-2026-26157: busybox 1.36.1 CVE-2026-26157 · CVSS 7.0 · EPSS 0.7% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-26157 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	busybox
High	CVE	CVE-2026-26158: busybox 1.36.1 CVE-2026-26158 · CVSS 7.0 · EPSS 0.2% (prioritisation signal; feed date not recorded for this row) · UNPROVEN Confidence: MEDIUM · Reachability evidence: Not recorded Fix: Update the affected library to a version that includes the security fix. Check the CVE's NVD page for the fixed version: https://nvd.nist.gov/vuln/detail/CVE-2026-26158 Yocto: update SRC_URI in your recipe to point to the patched version. Buildroot: update the package version in package/[pkg]/[pkg].mk. Confirm the upstream advisory, component identity and build recipe. Inspect the rebuilt artifact and run vulnerability-specific checks in an isolated authorized test environment. A version string alone does not verify remediation; do not execute recovered firmware on the analyst host.	busybox
High	ATTACK_SURFACE	UART debug shell on ttyS0 Confidence: HIGH · Reachability evidence: Not recorded Fix: Disable UART shell in etc/inittab. Comment out or remove the line spawning a shell on ttyS0. If UART is needed for diagnostics, require authentication before shell access. Reference: ETSI EN 303 645 Provision 5.6 - minimise exposed attack surfaces.	firmware-wide

Threat Model (HYBRID)

4/13	8	3
Properties confirmed present	Applicable threats	Critical-risk threats

Runtime (dynamic) evidence: Emulation ran (46/206 binaries ran), 0 reproduced crash(es), 2 observed behaviour(s), raising TID-202.

PID-271: Firmware cryptographic integrity validation SYSTEM SOFTWARE Not present
TID-211: Device Allows Unauthenticated Firmware Installation (critical, score 20) Update-path evidence shows images are installed without signature verification: lib/upgrade/fwtool.sh: fwtool_check_signature returns success when usr/bin/ucert is absent, and usr/bin/ucert is not in the image; remaining image checks are... Mitigate: Secure Firmware Update; Authenticate for Administrative Actions
PID-3231: Native binary execution restrictions APPLICATION SOFTWARE Not present

TID-301: Application Binaries Modified (critical, score 16)
97 of 191 binaries lack NX/DEP protections (51%).
Mitigate: Memory Hardening Against Code Injection; Secure Firmware Update
TID-327: Out of Bounds Memory Access (critical, score 16)
123 of 191 binaries lack stack-protector hardening.
Mitigate: Memory Hardening Against Code Injection; Process and Thread Memory Segmentation; Hardware Enforcement of Memory Access
PID-311: Web/HTTP application interface APPLICATION SOFTWARE Present
TID-320: SQL Injection (medium, score 8)
Web management configuration was identified. This property does not establish injection dataflow or deployed-device exposure; review the separately dated source-analysis findings.
Mitigate: Authenticate for Administrative Actions
TID-319: Cross Site Scripting (XSS) (medium, score 6)
Web management configuration was identified. This property does not establish injection dataflow or deployed-device exposure; review the separately dated source-analysis findings.
Mitigate: Authenticate for Administrative Actions
PID-41: Exposed remote network services NETWORKING Present
TID-202: Exploitable System Network Stack Component (medium, score 8)
1 binary(s) observed binding and listening under emulation (sandbox observations, not proof of deployed-device reachability); static attack-surface score 3.0.
Mitigate: Restrict Software Diagnostic Functions; Process and Thread Memory Segmentation
PID-411: Services handling sensitive information NETWORKING Not present
TID-411: Weak/Insecure Cryptographic Protocol (high, score 12)
4 weak-cryptography finding(s) identified.
Mitigate: Encrypt Network Traffic; Authenticate Network Messages
TID-408: Unencrypted Sensitive Data Communication (medium, score 9)
Plaintext service(s) detected: ['http'].
Mitigate: Encrypt Network Traffic; Secure Network Tunnels

Binary Hardening Matrix (191 binaries)

Binary	Arch	NX	PIE	RELRO	SP	Strip	Risk
dnsmasq	AARCH64	Yes	Yes	Full	Yes	Yes	10.0
busybox	AARCH64	Yes	No	Full	Yes	Yes	9.9
pppd	AARCH64	Yes	Yes	Full	Yes	Yes	8.3
procd	AARCH64	Yes	Yes	Full	Yes	Yes	8.3
libss.so.2.0	AARCH64	Yes	Yes	Full	No	Yes	8.1
ujail	AARCH64	Yes	Yes	Full	No	Yes	8.1
opkg	AARCH64	Yes	No	Full	Yes	Yes	8.0
uhttpd	AARCH64	Yes	Yes	Full	Yes	Yes	8.0
e2fsck	AARCH64	Yes	No	Full	Yes	Yes	7.8

netifd	AARCH64	Yes	No	Full	Yes	Yes	7.8
mke2fs	AARCH64	Yes	No	Full	Yes	Yes	7.8
kmodloader	AARCH64	Yes	No	Full	Yes	Yes	7.7
cgi-io	AARCH64	Yes	No	Full	Yes	Yes	7.7
libfstools.so	AARCH64	Yes	Yes	Full	Yes	Yes	7.7
libuci.so	AARCH64	Yes	Yes	Full	Yes	Yes	7.3
libext2fs.so.2.4	AARCH64	Yes	Yes	Full	Yes	Yes	7.3
libe2p.so.2.3	AARCH64	Yes	Yes	Full	Yes	Yes	7.3
rpcd	AARCH64	Yes	Yes	Full	Yes	Yes	7.3
ubusd	AARCH64	Yes	Yes	Full	Yes	Yes	6.9
utrace	AARCH64	Yes	Yes	Full	No	Yes	6.9
init	AARCH64	Yes	Yes	Full	Yes	Yes	6.5
pppoe.so	AARCH64	Yes	Yes	Full	Yes	Yes	6.3
libiwinfo.so.20230701	AARCH64	Yes	Yes	Full	Yes	Yes	6.3
libcom_err.so.0.0	AARCH64	Yes	Yes	Full	Yes	Yes	6.3
libblkid.so.1.1.0	AARCH64	Yes	Yes	Full	Yes	Yes	6.3
libnftables.so.1.1.0	AARCH64	Yes	Yes	Full	Yes	Yes	6.3
libuclient.so	AARCH64	Yes	Yes	Full	Yes	Yes	6.3
logread	AARCH64	Yes	No	Full	Yes	Yes	6.0
odhcp6c	AARCH64	Yes	No	Full	Yes	Yes	6.0
logd	AARCH64	Yes	No	Full	No	Yes	6.0
nft	AARCH64	Yes	No	Full	No	Yes	6.0
uci	AARCH64	Yes	No	Full	No	Yes	6.0
uclient-fetch	AARCH64	Yes	No	Full	Yes	Yes	5.4
usign	AARCH64	Yes	No	Full	Yes	Yes	5.4
px5g	AARCH64	Yes	No	Full	Yes	Yes	5.4
odhcpd	AARCH64	Yes	Yes	Full	Yes	Yes	5.4
blkid	AARCH64	Yes	No	Full	Yes	Yes	5.4

partx	AARCH64	Yes	No	Full	Yes	Yes	5.4
jsonfilter	AARCH64	Yes	No	Full	Yes	Yes	5.4
dropbear	AARCH64	Yes	Yes	Full	Yes	Yes	5.2
libubus.so.20230605	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
libblobmsg_json.so.20230523	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
luci.so	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
libsmartcols.so.1.1.0	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
rrdns.so	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
libjson_script.so.20230523	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
libvalidate.so	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
file.so	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
libucode.so.20230711	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
libubox.so.20230523	AARCH64	Yes	Yes	Full	Yes	Yes	4.2
mkfs.f2fs	AARCH64	Yes	No	Full	No	Yes	3.6
mount_root	AARCH64	Yes	No	Full	No	Yes	3.6
jffs2reset	AARCH64	Yes	No	Full	No	Yes	3.6
validate_data	AARCH64	Yes	No	Full	No	Yes	3.6
libpreload-seccomp.so	AARCH64	Yes	Yes	Full	No	Yes	3.6
mtd	AARCH64	Yes	No	Full	Yes	Yes	3.6
jshn	AARCH64	Yes	No	Full	Yes	Yes	2.4
getrandom	AARCH64	Yes	No	Full	Yes	Yes	2.4
libmnl.so.0.2.0	AARCH64	Yes	Yes	Full	No	Yes	2.4
math.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
lucihttp.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
addpart	AARCH64	Yes	No	Full	Yes	Yes	2.4
delpart	AARCH64	Yes	No	Full	Yes	Yes	2.4
ucode	AARCH64	Yes	No	Full	Yes	Yes	2.4
fwtool	AARCH64	Yes	No	Full	Yes	Yes	2.4

luci-bwc	AARCH64	Yes	No	Full	Yes	Yes	2.4
libjansson.so.4.14.0	AARCH64	Yes	Yes	Full	No	Yes	2.4
liblucihttp.so.0.1	AARCH64	Yes	Yes	Full	No	Yes	2.4
ubus.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
udevtrigger	AARCH64	Yes	Yes	Full	No	Yes	2.4
askfirst	AARCH64	Yes	Yes	Full	No	Yes	2.4
libc.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
libpreload-trace.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
libgcc_s.so.1	AARCH64	Yes	Yes	Full	No	Yes	2.4
libsetlbf.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
libustream-ssl.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
urngd	AARCH64	Yes	No	Full	Yes	Yes	2.4
uhttpd_ubus.so	AARCH64	Yes	Yes	Full	No	Yes	2.4
fs.so	AARCH64	Yes	Yes	Full	Yes	Yes	2.4
ubus	AARCH64	Yes	Yes	Full	No	Yes	2.4
nft_ct.ko	AARCH64	No	No	None	No	No	0.9
smisc.ko	AARCH64	No	No	None	No	No	0.9
xgmac_mdio.ko	AARCH64	No	No	None	No	No	0.9
bcm-phy-lib.ko	AARCH64	No	No	None	No	No	0.9
nft_counter.ko	AARCH64	No	No	None	No	No	0.9
vmxnet3.ko	AARCH64	No	No	None	No	No	0.9
rvu_af.ko	AARCH64	No	No	None	No	No	0.9
realtek.ko	AARCH64	No	No	None	No	No	0.9
nf_tables.ko	AARCH64	No	No	None	No	No	0.9
nft_fib_ipv6.ko	AARCH64	No	No	None	No	No	0.9
i2c-mux-pca954x.ko	AARCH64	No	No	None	No	No	0.9
nicpf.ko	AARCH64	No	No	None	No	No	0.9
rtc-rx8025.ko	AARCH64	No	No	None	No	No	0.9

stmmac-platform.ko	AARCH64	No	No	None	No	No	0.9
slhc.ko	AARCH64	No	No	None	No	No	0.9
seqiv.ko	AARCH64	No	No	None	No	No	0.9
nft_masq.ko	AARCH64	No	No	None	No	No	0.9
nft_fib_inet.ko	AARCH64	No	No	None	No	No	0.9
nf_nat.ko	AARCH64	No	No	None	No	No	0.9
drbg.ko	AARCH64	No	No	None	No	No	0.9
pcs_xpcs.ko	AARCH64	No	No	None	No	No	0.9
pppoe.ko	AARCH64	No	No	None	No	No	0.9
jitterentropy_rng.ko	AARCH64	No	No	None	No	No	0.9
marvell10g.ko	AARCH64	No	No	None	No	No	0.9
nft_quota.ko	AARCH64	No	No	None	No	No	0.9
crc-ccitt.ko	AARCH64	No	No	None	No	No	0.9
dwmac-generic.ko	AARCH64	No	No	None	No	No	0.9
aquantia.ko	AARCH64	No	No	None	No	No	0.9
nft_nat.ko	AARCH64	No	No	None	No	No	0.9
nf_flow_table_ipv6.ko	AARCH64	No	No	None	No	No	0.9
ppp_generic.ko	AARCH64	No	No	None	No	No	0.9
nft_reject.ko	AARCH64	No	No	None	No	No	0.9
lzo_compress.ko	AARCH64	No	No	None	No	No	0.9
mdio-gpio.ko	AARCH64	No	No	None	No	No	0.9
libcrc32c.ko	AARCH64	No	No	None	No	No	0.9
marvell.ko	AARCH64	No	No	None	No	No	0.9
nf_defrag_ipv6.ko	AARCH64	No	No	None	No	No	0.9
nf_reject_ipv6.ko	AARCH64	No	No	None	No	No	0.9
nicvf.ko	AARCH64	No	No	None	No	No	0.9
fec.ko	AARCH64	No	No	None	No	No	0.9
hmac.ko	AARCH64	No	No	None	No	No	0.9

nft_numgen.ko	AARCH64	No	No	None	No	No	0.9
nft_reject_ipv6.ko	AARCH64	No	No	None	No	No	0.9
ptp.ko	AARCH64	No	No	None	No	No	0.9
fsl-enetc-ierb.ko	AARCH64	No	No	None	No	No	0.9
ravb.ko	AARCH64	No	No	None	No	No	0.9
nf_reject_ipv4.ko	AARCH64	No	No	None	No	No	0.9
hwmon.ko	AARCH64	No	No	None	No	No	0.9
nft_limit.ko	AARCH64	No	No	None	No	No	0.9
fsl-dpaa2-eth.ko	AARCH64	No	No	None	No	No	0.9
nft_chain_nat.ko	AARCH64	No	No	None	No	No	0.9
fsl-enetc.ko	AARCH64	No	No	None	No	No	0.9
dwmac-sun8i.ko	AARCH64	No	No	None	No	No	0.9
mdio-thunder.ko	AARCH64	No	No	None	No	No	0.9
thunder_bgx.ko	AARCH64	No	No	None	No	No	0.9
atlantic.ko	AARCH64	No	No	None	No	No	0.9
dwmac-imx.ko	AARCH64	No	No	None	No	No	0.9
pps_core.ko	AARCH64	No	No	None	No	No	0.9
nls_iso8859-1.ko	AARCH64	No	No	None	No	No	0.9
nf_flow_table.ko	AARCH64	No	No	None	No	No	0.9
macsec.ko	AARCH64	No	No	None	No	No	0.9
nls_utf8.ko	AARCH64	No	No	None	No	No	0.9
nft_objref.ko	AARCH64	No	No	None	No	No	0.9
nft_reject_inet.ko	AARCH64	No	No	None	No	No	0.9
rvu_nicvf.ko	AARCH64	No	No	None	No	No	0.9
nf_conntrack.ko	AARCH64	No	No	None	No	No	0.9
lzo.ko	AARCH64	No	No	None	No	No	0.9
sfp.ko	AARCH64	No	No	None	No	No	0.9
nft_fib_ipv4.ko	AARCH64	No	No	None	No	No	0.9

rvu_mbox.ko	AARCH64	No	No	None	No	No	0.9
mdio-cavium.ko	AARCH64	No	No	None	No	No	0.9
nls_cp437.ko	AARCH64	No	No	None	No	No	0.9
vfat.ko	AARCH64	No	No	None	No	No	0.9
mii.ko	AARCH64	No	No	None	No	No	0.9
gpio-pca953x.ko	AARCH64	No	No	None	No	No	0.9
phylink.ko	AARCH64	No	No	None	No	No	0.9
fsl-mc-dpio.ko	AARCH64	No	No	None	No	No	0.9
i2c-dev.ko	AARCH64	No	No	None	No	No	0.9
fat.ko	AARCH64	No	No	None	No	No	0.9
mvpp2.ko	AARCH64	No	No	None	No	No	0.9
nf_log_syslog.ko	AARCH64	No	No	None	No	No	0.9
nft_hash.ko	AARCH64	No	No	None	No	No	0.9
nf_flow_table_inet.ko	AARCH64	No	No	None	No	No	0.9
nft_flow_offload.ko	AARCH64	No	No	None	No	No	0.9
pppox.ko	AARCH64	No	No	None	No	No	0.9
nft_log.ko	AARCH64	No	No	None	No	No	0.9
e1000e.ko	AARCH64	No	No	None	No	No	0.9
sha512_generic.ko	AARCH64	No	No	None	No	No	0.9
dwmac-rk.ko	AARCH64	No	No	None	No	No	0.9
lzo-rle.ko	AARCH64	No	No	None	No	No	0.9
lzo_decompress.ko	AARCH64	No	No	None	No	No	0.9
pcs-lynx.ko	AARCH64	No	No	None	No	No	0.9
i2c-mux.ko	AARCH64	No	No	None	No	No	0.9
thunder_xcv.ko	AARCH64	No	No	None	No	No	0.9
stmmac.ko	AARCH64	No	No	None	No	No	0.9
mvneta.ko	AARCH64	No	No	None	No	No	0.9
rvu_nicpf.ko	AARCH64	No	No	None	No	No	0.9

libmbedcrypto.so.2.28.9	AARCH64	Yes	Yes	Full	Yes	Yes	0.3
libmbedtls.so.2.28.9	AARCH64	Yes	Yes	Full	Yes	Yes	0.3
uci.so	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
libf2fs.so.10.0.0	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
libuuid.so.1.3.0	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
html.so	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
core.so	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
libmbedx509.so.2.28.9	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
ucode.so	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
upgraded	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
libnl-tiny.so.1	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
libnftnl.so.11.6.0	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
libjson-c.so.5.2.0	AARCH64	Yes	Yes	Full	Yes	Yes	0.0
iwinfo.so	AARCH64	Yes	Yes	Full	Yes	Yes	0.0

Network Attack Surface

Service	Port	Protocol	Risk	Source
SSH	22	TCP	Medium	etc/config/dropbear
HTTP	80	TCP	Medium	etc/init.d/uhttpd

Attack surface score: 3.0 / 10 · Plaintext services: http · Debug interfaces: None

Software Bill of Materials (33 components)

Library	Version	PURL	CVEs	Critical
busybox	1.36.1	pkg:generic/busybox@1.36.1	20	0
dnsmasq	2.90	pkg:generic/dnsmasq@2.90	11	0
dropbear	2022.82	pkg:generic/dropbear@2022.82	2	0
libblkid.so.1	-	pkg:generic/blkid?soname=libblkid.so.1	0	0
libblobmsg_json.so.20230523	-	pkg:generic/blobmsg_json?soname=libblobmsg_json.so.20230523	0	0
libcom_err.so.0	-	pkg:generic/com_err?soname=libcom_err.so.0	0	0

libc.so	-	pkg:generic/c?soname=libc.so	0	0
libe2p.so.2	-	pkg:generic/e2p?soname=libe2p.so.2	0	0
libext2fs.so.2	-	pkg:generic/ext2fs?soname=libext2fs.so.2	0	0
libf2fs.so.10	-	pkg:generic/f2fs?soname=libf2fs.so.10	0	0
libfstools.so	-	pkg:generic/fstools?soname=libfstools.so	0	0
libgcc_s.so.1	-	pkg:generic/gcc?soname=libgcc_s.so.1	0	0
libiwinfo.so.20230701	-	pkg:generic/iwinfo?soname=libiwinfo.so.20230701	0	0
libjansson.so.4	-	pkg:generic/jansson?soname=libjansson.so.4	0	0
libjson-c.so.5	-	pkg:generic/json-c?soname=libjson-c.so.5	0	0
libjson_script.so.20230523	-	pkg:generic/json_script?soname=libjson_script.so.20230523	0	0
liblucihttp.so.0	-	pkg:generic/lucihttp?soname=liblucihttp.so.0	0	0
libmbedcrypto.so.7	-	pkg:generic/mbedtls?soname=libmbedcrypto.so.7	0	0
libmbedtls.so.14	-	pkg:generic/mbedtls?soname=libmbedtls.so.14	0	0
libmbedtls509.so.1	-	pkg:generic/mbedtls?soname=libmbedtls509.so.1	0	0
libmnl.so.0	-	pkg:generic/mnl?soname=libmnl.so.0	0	0
libnftables.so.1	-	pkg:generic/nftables?soname=libnftables.so.1	0	0
libnftnl.so.11	-	pkg:generic/nftnl?soname=libnftnl.so.11	0	0
libnl-tiny.so.1	-	pkg:generic/nl-tiny?soname=libnl-tiny.so.1	0	0
libsmartcols.so.1	-	pkg:generic/smartcols?soname=libsmartcols.so.1	0	0
libubox.so.20230523	-	pkg:generic/ubox?soname=libubox.so.20230523	0	0
libubus.so.20230605	-	pkg:generic/ubus?soname=libubus.so.20230605	0	0
libuci.so	-	pkg:generic/uci?soname=libuci.so	0	0
libuclient.so	-	pkg:generic/uclient?soname=libuclient.so	0	0
libucode.so.20230711	-	pkg:generic/ucode?soname=libucode.so.20230711	0	0
libuuid.so.1	-	pkg:generic/uuid?soname=libuuid.so.1	0	0
libvalidate.so	-	pkg:generic/validate?soname=libvalidate.so	0	0
openwrt	23.05.5	pkg:generic/openwrt@23.05.5	23	6

separate manual assessment.