

Readiness report — FarmBot Open-Source Farming Robot

Checked 2026-09-03 15:52 · 88 searches, 18 pages fetched

Readiness: FarmBot Open-Source Farming Robot

Verdict: Ready with caveats · 2026-09-03 · est. parts cost \$13.28-\$75.00 (controller board only; the host server is unpriced and no electromechanical BOM was uploaded)

Cybersecurity — software & network: Do not place on an open network

This is the cold check for this lab — it establishes the baseline every future report will measure drift against. Every part the snapshot actually lists is easy to buy today and none is anywhere near end of production: all three Raspberry Pi controller options carry Raspberry Pi obsolescence statements running to 2030 or 2034, bare boards run \$13.28 to \$75.00 depending on which target you build for, and the host server is ordinary commodity hardware or a cloud instance. Nothing needed a substitute. The verdict is not a clean "Ready" for two reasons. First, this upload is the FarmBot software tree only: it contains no schematics, board files, Gerbers or parts list for the machine itself, so the motors, motor drivers, encoders, solenoid valves, gantry extrusions and power distribution that make a FarmBot move were never in scope and cannot be called ready or not ready. Second, the host machine is deliberately left unpriced because no specific machine or instance was chosen. An instructor can stand up the control software from these materials; they cannot build the robot from them.

Action required

None — all checked parts are sourceable.

Cybersecurity — software & network

Do not place on an open network — The device firmware runs on an end-of-life Erlang runtime with no fix path, ships a publicly known remote-connection secret alongside an enabled SSH daemon, and carries several high-severity flaws in the web stack it exposes on the network.

Component	Version	How known	Support status
FarmBot OS (device firmware)	15.5.2	read from project (VERSION file in the farmbot_os repository (fetched/08-VERSION))	—

Component	Version	How known	Support status
Elixir	1.16.2	read from project (.tool-versions (fetched/06-.tool-versions); ELIXIR_VERSION states the range ~> 1.16.2)	supported
Erlang/OTP	26.2.5	read from project (.tool-versions (fetched/06-.tool-versions))	unsupported since 2026-05-26
Nerves system targets (farmbot_system_rpi / rpi3 / rpi4)	v1.23.1-farmbot.1	inferred (git tag declared in mix.exs; mix.lock pins commits f3d3f1da4ca9 / 12835da22dd5 / 09062dde96d6)	—
cowboy (device HTTP server)	2.12.0	read from project (mix.lock (fetched/04-mix.lock); transitive under plug_cowboy)	—
cowlib	2.13.0	read from project (mix.lock (fetched/04-mix.lock))	—
plug	1.15.3	read from project (mix.lock (fetched/04-mix.lock))	—
plug_cowboy	2.7.1	read from project (mix.lock; mix.exs declares the constraint ~> 2.7)	—
tesla (device HTTP client)	1.9.0	read from project (mix.lock; mix.exs declares the constraint ~> 1.9)	—
hackney (HTTP transport under tesla)	1.20.1	read from project (mix.lock; mix.exs declares the constraint ~> 1.20)	—
decimal	2.1.1	read from project (mix.lock; transitive under ecto)	—
tortoise311 (device MQTT client)	0.11.7	read from project (mix.lock (fetched/04-mix.lock))	—
vintage_net_wifi	0.12.5	read from project (mix.lock (fetched/04-mix.lock))	—
mdns_lite (local network discovery)	0.8.8	read from project (mix.lock (fetched/04-mix.lock))	—
cors_plug	3.0.3	read from project (mix.lock (fetched/04-mix.lock))	—
nerves_runtime	0.13.6	read from project (mix.lock (fetched/04-mix.lock))	—
Ruby (web app runtime)	4.0.6	read from project (.ruby-version (fetched/09-.ruby-version) and the RUBY VERSION block of Gemfile.lock)	supported until 2029-03-31

Component	Version	How known	Support status
Ruby on Rails	8.1.3.1	read from project (Gemfile.lock (fetched/01-Gemfile.lock); the Gemfile itself declares no constraint)	—
Devise (web app authentication)	5.0.4	read from project (Gemfile.lock (fetched/01-Gemfile.lock))	—
Phusion Passenger (application server)	6.2.0	read from project (Gemfile.lock (fetched/01-Gemfile.lock))	—
nokogiri	1.19.4	read from project (Gemfile.lock pins eight platform-specific builds of 1.19.4)	—
PostgreSQL	17	read from project (docker-compose.yml pins the image postgres:17 (fetched/10-docker-compose.yml))	supported until 2029-11-08
Valkey (Redis-compatible cache)	9.0	read from project (docker-compose.yml pins the image valkey/valkey:9.0 (fetched/10-docker-compose.yml))	—
RabbitMQ / MQTT broker	not determined	not determined (docker-compose.yml builds it from docker_configs/rabbitmq.Dockerfile, which was not fetched, so no version is on record)	—
Bun (frontend toolchain and runtime)	not determined	unpinned (package.json declares packageManager bun@1.x, a range rather than a pin)	—
React (web frontend)	19.2.8	read from project (package.json (fetched/03-package.json))	—
TypeScript	6.0.3	read from project (package.json; the @typescript/native entry additionally aliases typescript 7.0.2, which was checked separately)	—

Component	Finding	Severity	Fix available?
cowboy 2.12.0	The web server FarmBot OS runs on the Raspberry Pi can be driven into denial of service by malformed multipart or duplicated headers, and used for HTTP request and response splitting, by anyone who can reach its port. — GHSA-jfc2-q6qh-g5x8 , GHSA-w4f7-4cxr-rv3c , EEF-CVE-2026-65624	high	Yes — update to 2.18.0

Component	Finding	Severity	Fix available?
cowlib 2.13.0	The protocol library beneath the device's web server can be made to exhaust the Raspberry Pi's memory with a single crafted compressed or oversized-header request, and allows CRLF and cookie injection. — GHSA-84f2-rp86-235p , GHSA-32p9-57cr-4x65 , GHSA-hv23-4qp7-8c8r , GHSA-g2wm-735q-3f56 (+2 more)	high	Mitigation only — updating to 2.19.0 clears four of the seven; three have no fixed release, so keep the device off untrusted networks
hackney 1.20.1	The HTTP transport underneath the device's web client has a server-side request forgery bypass, header injection, and a TLS upgrade with no timeout that can hang a connection indefinitely. — GHSA-gp9c-pm5m-5cxc , GHSA-j9wq-vxxc-94wf , GHSA-pj7v-xfvx-wmjg , GHSA-vq52-99r9-h5pw (+2 more)	high	No — project pins hackney ~> 1.20 in mix.exs; the fixes for the high-severity issues ship in 4.0.1
plug 1.15.3	The device's request-handling layer can be exhausted by multipart uploads and deeply nested query parameters, and allows cookie attribute injection, all reachable without logging in. — GHSA-468c-vq7p-gh64 , EEF-CVE-2026-56813 , EEF-CVE-2026-56814 , EEF-CVE-2026-54892	high	Yes — update to 1.19.5
plug_cowboy 2.7.1	An unauthenticated attacker on the same network can crash the device's web server with HTTP/2 requests that exhaust the Erlang atom table. — GHSA-q8x4-x7mp-5vg2	high	Yes — update to 2.8.1
tesla 1.9.0	The HTTP client the device uses to reach the web app leaks its Authorization header when a request is redirected to another origin, and can be crashed by an oversized compressed response. — GHSA-9m9w-gxf7-rh8m , GHSA-h74c-q9j7-mpcm , GHSA-mc85-72gr-vm9f , GHSA-28jh-g32x-v9v4 (+1 more)	high	Yes — update to 1.18.3
decimal 2.1.1	A number with an oversized exponent makes this library allocate without bound, which an unauthenticated request carrying such a value could trigger on the device. — GHSA-rhv4-8758-jx7v	moderate	Mitigation only — the fix is decimal 3.0.0, a major bump pulled in transitively through ecto; verify ecto compatibility before updating
nokogiri 1.19.4	Eight XML-parsing advisories match the platform-specific nokogiri builds pinned in Gemfile.lock, but every one of them names 1.19.4 as its fixed version, the same release the lockfile pins, so this most likely reflects how platform suffixes sort rather than a live exposure. — GHSA-5prv-v3j2-97mh , GHSA-8678-w3jw-xfc2 , GHSA-5v8h-3h3q-446p , GHSA-9cv2-cfxc-v4v2 (+2 more)	moderate	Mitigation only — confirm the installed nokogiri build reports 1.19.4 or later; no upgrade beyond the current pin is indicated

Component	Finding	Severity	Fix available?
Erlang/OTP 26.2.5	The device firmware is built on Erlang/OTP 26, whose support ended on 2026-05-26, so no further security fixes are published for the runtime that FarmBot OS itself runs on.	posture	No — requires platform migration
FarmBot OS release configuration	The firmware ships a hardcoded Erlang distribution cookie, the literal string 'democookie' (mix.exs line 63), and enables the Erlang SSH daemon (:ssh in extra_applications, mix.exs line 90); that cookie is the shared secret authorising a remote connection to the running node, and it is published in the source for anyone to read.	posture	Mitigation only — set a unique release cookie before building firmware and keep the device on an isolated network segment
Self-hosted web app broker (docker-compose)	The self-hosted stack publishes the message broker straight to the host: ports 1883 (plaintext MQTT), 8883, 5672 (AMQP), 3002 (MQTT over WebSockets) and 15672 (the RabbitMQ management web interface), so anything that can route to the server can reach all of them.	posture	Mitigation only — bind these ports to localhost or a private interface and firewall the host; never expose 1883 or 15672 to a campus or public network
Web app Gemfile	49 of the 50 gems in the web app's Gemfile carry no version constraint at all, so a bundle update can move the entire Rails stack without review; the committed Gemfile.lock does pin all 184 resolved gems and is what was checked here.	posture	Mitigation only — install from the committed Gemfile.lock (bundle install --deployment) and review any bundle update

What this means for your lab

Treat this as equipment that must not sit on a shared campus or public network. The FarmBot controller runs a web server and an SSH service on the Raspberry Pi, and the firmware ships with a published connection secret (the literal word 'democookie') that is meant to be replaced before you build an image; leave it as shipped and anyone who can reach the device on the network can attach to the software running it and command the machine. The device's web and HTTP libraries also have known flaws that let a stranger crash it with a single malformed request, and the Erlang runtime it is built on stopped receiving security fixes in May 2026, so those will not be patched for you. If you self-host the web app, the default compose file also opens the message broker and its administration web page directly to the network. What to do: put the FarmBot and its server on their own isolated network segment or VLAN with no inbound access from outside, set your own release cookie and your own admin, database and Devise secrets before deploying, install the Ruby side from the committed lockfile rather than letting it pull the newest gems, and talk to campus IT before connecting any of it to the institutional network. Nothing here means the software is unusable in a lab - it means it should be run on a network you control.

Not checked

- FarmBot Web App frontend transitive dependencies (bun.lock): bun.lock is not a lockfile format this pipeline parses; only the 95 direct pins in package.json were checked
- RabbitMQ / MQTT broker image: version not determined - the compose file builds it from docker_configs/rabbitmq.Dockerfile, which was not fetched
- Bun runtime: unpinned - package.json declares bun@1.x, a range, so there is no version to check
- farmbot_system_rpi / farmbot_system_rpi3 / farmbot_system_rpi4: source-hosted GitHub dependencies pinned by git tag and commit; no package registry and no advisory database covers them
- Linux kernel and Buildroot userland inside the Nerves firmware images: the built firmware images were not fetched or unpacked, so only the Elixir and Erlang layer above them was checked
- Ubuntu Server (host operating system): no version is stated anywhere in the project or the snapshot, so no support-status lookup was possible
- example.env: not a dependency manifest - the parser classified this environment-variable template as a requirements file, so its 60 rows are variable names, not packages, and no versions were checked from it

Parts

Bill of Materials

Part	Spec/Package	Status	Stock	Price	Source
Raspberry Pi 4 Model B (RPI 4 target)	SBC 85 × 56 mm, BCM2711, 5.0–5.25 V DC ≥ 3.0 A via USB-C, 3.3 V GPIO; 2/4/8 GB all acceptable for farmbot_system_rpi4	readily available; production guaranteed to 01 Jan 2034	not stated by retail listings	\$55.00 · (2 GB) · \$75.00 · (8 GB)	PiShop USA (2 GB), CanaKit.com (8 GB)
Raspberry Pi 3 Model B / B+ (RPI 3 target)	SBC 85 × 56 mm, BCM2837/BCM2837B0, 5.0–5.25 V DC ≥ 2.5 A via Micro-USB, 3.3 V GPIO; farmbot_system_rpi3	readily available; B+ production guaranteed to 01 Jan 2030 (plain 3 Model B ends 01 Jan 2028 — prefer the B+)	not stated by retail listings	\$40.00 · \$52.59	PiShop USA, Best Buy

Part	Spec/Package	Status	Stock	Price	Source
Raspberry Pi Zero W / Zero WH (RPI 1 / Zero target)	SBC 65 × 30 mm, BCM2835 ARMv6, 5.0 V DC ≥ 1.2 A via Micro-USB, 3.3 V GPIO; <code>farmbot_system_rpi</code>	readily available; Zero W/WH production guaranteed to 01 Jan 2030	not stated by retail listings	\$13.28 · \$15.00 · \$16.00 (Zero WH)	JAK Electronics, Seeed Studio
Raspberry Pi 1 Model B+ (same RPi 1 / Zero target, wired only)	SBC 85 × 56 mm, BCM2835 ARMv6, 512 MB; named on this BOM line by the snapshot; no Wi-Fi	readily available; production guaranteed to 01 Jan 2030	not stated by retail listing	\$25.00	DigiKey
Host Application Server Machine	Generic x86_64 Linux host or cloud VM; ≥ 2 cores, 4 GB RAM; Ubuntu Server with Docker, Ruby, PostgreSQL	readily available (commodity); price not checked — no specific machine or instance chosen	—	—	—
Electromechanical BOM (motors, motor drivers, encoders, solenoid valves, gantry extrusions, power distribution)	—	not checked	—	—	—

Two near-match traps appeared in the shopping results and are recorded here so a future check does not mistake them for price movement. The \$25.00 DigiKey listing "Raspberry Pi Model B+ 512MB RAM" surfaced under the Pi 3 Model B+ search but is the 2014 Pi 1 Model B+ — a different board, priced in its own row above. And the "Raspberry Pi Zero 2 W" listings at \$18.00 and \$28.93 surfaced under the Zero W search; the snapshot restricts that BOM line to the ARMv6 BCM2835 architecture the `farmbot_system_rpi` target builds for, so the Zero 2 W is out of spec, not a cheaper equivalent.

Substitutes

None needed.

Other dependencies

- **No hardware design files at all.** The snapshot's own fabrication section records no board layer count and no board dimensions because no PCB CAD, Gerber, drill or fabrication files were uploaded. Downstream checking of the physical build — motor drivers, rotary encoders, solenoid valves, power distribution — cannot be performed from these materials. This is the single largest gap in the report.

- **Historical OS releases**, https://github.com/FarmBot/farmbot_os/releases — fetched this session and readable. The release list is live and current: newest entries v15.5.3-rc1 and v15.5.2, which matches the 15.5.2 in the repository's own VERSION file, so the download channel the lab depends on is alive and in step with the source tree.
- **OS image downloads**, <https://my.farm.bot/os> — fetched this session; the page downloaded but returned no extractable text (it is JavaScript-rendered). Reachable; content not checked.
- **Official documentation**, <https://software.farm.bot/docs/farmbot-os> — fetched this session; downloaded but no extractable text. Reachable; content not checked.
- **Vendor host-machine specification**, <https://raw.githubusercontent.com/FarmBot/Farmbot-Web-App/main/DEPLOYMENT.md> — fetched this session; returned no extractable text, so FarmBot's own stated minimum host spec is not checked. The "≥ 2 cores, 4 GB RAM" figure in the Parts table is the snapshot's, not the vendor's.
- **Further farm.bot properties listed in the snapshot** — <https://developer.farm.bot/docs/farmbot-os>, <https://developer.farm.bot/docs/api-docs>, <https://software.farm.bot/docs/getting-started>, <https://my.farm.bot/>, <http://disclosure.farm.bot/> and <https://farm.bot/responsible-disclosure-of-security-vulnerabilities/>: not checked, no fetch attempted this run. All sit on the same two hosts as the two pages above, which did respond.

Watch list

- **The missing electromechanical BOM.** Until the lab's hardware files are uploaded, every re-check will keep reporting the same three Raspberry Pi boards and nothing about the machine. Getting the parts list into the lab materials is worth more than any sourcing action in this report.
- **Raspberry Pi Zero W / Pi 1 Model B+ (the ARMv6 target).** These are the oldest boards in the list and the ones a supplier is most likely to quietly swap for a Zero 2 W, which the `farmbot_system_rpi` build does not target. Check what actually arrives, and watch for the 01 Jan 2030 end-of-production date coming into view.
- **Raspberry Pi 3 Model B+.** Now priced at or above a Pi 4 2 GB in several listings, so its cost advantage is gone; if that persists, standardising on the Pi 4 target is the cheaper and longer-lived choice (2034 versus 2030).
- **Retail-only pricing.** All three boards were priced from consumer shopping listings rather than an authorized distributor catalog, so stock levels are unknown and prices move faster than distributor pricing. Expect noisier drift on these rows than on a typical BOM.
- **Host server sizing.** Unpriced this run by design. Once a specific machine or cloud instance is chosen, record it so the next check has a baseline.