

Readiness report — Public Lab Desktop Spectrometry Kit

Checked 2026-09-03 03:04 · 7 searches, 11 pages fetched

Readiness: Public Lab Desktop Spectrometry Kit

Verdict: Ready with caveats · 2026-09-03 · est. parts cost \$31–\$86 (four purchased lines; cardstock and laser cutting not priced) **Cybersecurity — software & network: Do not place on an open network**

This is the cold check for this lab — there is no previous report, so this one establishes the baseline every future check will measure drift against. Every purchasable item in the bill of materials is in stock today from multiple sellers, and both laser-cut enclosure files are still served from the project's GitHub repository. Two things keep this off a clean "Ready". First, publiclab.org served nothing to the checker: the 0.2 mm slit-card cut template and the whole body of assembly and calibration notes the lab leans on could not be verified this run, and whether that is a bot block or an outage was not established — verify by hand. Second, no single product listing verifies both manual focus and enclosure fit for the webcam, so the specific model you order needs a look before you buy a class set. Neither is a sourcing failure: every part here is cheap, commodity, and available from several sellers at once.

Action required

Part	Problem	Recommended action
Precision Slit Card (0.2 mm)	The Public Lab note holding the cut template (publiclab.org/n/11246) could not be downloaded by the checker — "blocked, timeout, or gone"	Open the note in a browser to confirm it is reachable and save the template locally. Nothing needs purchasing: the snapshot allows any rigid opaque substrate with a 0.2 mm slit
Focus-Adjustable USB Webcam Module	No listing verifies manual focus and fit in the 35 mm enclosure compartment together	Before a bulk order, buy one unit and confirm the lens focuses manually at a 200 mm object distance and the housing fits (or comes off)

Cybersecurity — software & network

Do not place on an open network — The runtime is past end of life and the pinned Rails 5.2.4.6 carries critical remote-code-execution advisories on the web application students connect to, with the fix blocked by the project's own rails ~> 5.2.4.3 constraint.

Component	Version	How known	Support status
Host operating system (Ubuntu / Debian Linux)	18.04	inferred (Snapshot records Ubuntu 18.04 LTS as the documented target; the fetched README (fetched/03-README.md line 35) says only 'for an Ubuntu/Debian system' with no version.)	extended/LTS support only until 2028-04-26
Ruby language runtime	2.6.6	read from project (fetched/03-README.md line 31 ('The app now runs on Ruby 2.6.6 up to Ruby 2.6.x') and line 58 ('rvm install 2.6.6').)	unsupported since 2022-03-31
Ruby on Rails	5.2.4.6	read from project (fetched/01-Gemfile.lock; the Gemfile declares 'gem "rails", "~> 5.2.4.3"' (fetched/02-Gemfile line 5).)	—
Bundler	1.17.2	read from project (fetched/01-Gemfile.lock lines 280-281, 'BUNDLED WITH 1.17.2'.)	—
Puma (application server)	5.6.4	read from project (fetched/01-Gemfile.lock line 127; the Gemfile declares 'gem "puma"' with no version constraint (fetched/02-Gemfile line 17).)	—
Phusion Passenger (application server)	6.0.14	read from project (fetched/01-Gemfile.lock; the Gemfile declares 'gem "passenger"' with no version constraint (fetched/02-Gemfile line 38).)	—
Rack (web server interface)	2.2.4	read from project (fetched/01-Gemfile.lock line 130; required as 'rack (~> 2.0, >= 2.0.8)' at line 17.)	—
Nokogiri (XML/HTML parser)	1.13.8	read from project (fetched/01-Gemfile.lock line 107; required as 'nokogiri (~> 1.8)' at lines 56 and 239.)	—
rails-html-sanitizer (HTML sanitisation)	1.4.3	read from project (fetched/01-Gemfile.lock line 160; required as 'rails-html-sanitizer (~> 1.0, >= 1.0.2)' at line 20.)	—
loofah (HTML sanitisation)	2.18.0	read from project (fetched/01-Gemfile.lock line 86; required as 'loofah (~> 2.3)' at line 161.)	—
REXML (XML parser)	3.2.5	read from project (fetched/01-Gemfile.lock line 182; required as 'rexml (>= 3.2.5, < 4.0)' at line 190.)	—

Component	Version	How known	Support status
RMagick (image processing binding)	4.2.6	read from project (fetched/01-Gemfile.lock; the Gemfile declares 'gem "rmagick"' with no version constraint (fetched/02-Gemfile line 42).)	—
rdiscount (Markdown renderer)	2.2.0.2	read from project (fetched/01-Gemfile.lock; the Gemfile pins it exactly as 'gem "rdiscount", "2.2.0.2"' (fetched/02-Gemfile line 47).)	—
mysql2 (database driver)	0.5.4	read from project (fetched/01-Gemfile.lock; the Gemfile declares 'gem "mysql2", "~> 0.5.4"' (fetched/02-Gemfile line 9).)	—
paperclip (file attachments)	6.1.0	read from project (fetched/01-Gemfile.lock.)	—
recaptcha	5.9.0	read from project (fetched/01-Gemfile.lock; the Gemfile pins 'gem "recaptcha", "5.9.0"' (fetched/02-Gemfile line 39).)	—
open_id_authentication (student login via publiclab.org)	1.3.0	read from project (fetched/01-Gemfile.lock; declared as 'gem "open_id_authentication" at fetched/02-Gemfile line 53.)	—
ruby-openid (student login via publiclab.org)	2.9.2	read from project (fetched/01-Gemfile.lock line 199; declared as 'gem "ruby-openid" at fetched/02-Gemfile line 55.)	—
therubyracer (JavaScript runtime)	0.12.3	read from project (fetched/01-Gemfile.lock.)	—
uglifier (asset minifier)	4.2.0	read from project (fetched/01-Gemfile.lock.)	—
bootsnap	1.12.0	read from project (fetched/01-Gemfile.lock.)	—
sprockets (asset pipeline)	4.1.1	read from project (fetched/01-Gemfile.lock.)	—
ImageMagick and development headers (imagemagick, ruby-rmagick, libmagickwand-dev, libmagick++-dev)	not determined	unpinned (Installed by apt with no version: fetched/03-README.md line 43.)	—
Node.js, npm and Yarn (static assets)	not determined	unpinned (Installed with no version: fetched/03-README.md lines 64-72 ('apt-get install nodejs-legacy', 'npm install -g yarn').)	—

Component	Version	How known	Support status
Database engine (MySQL Server or SQLite3)	not determined	unpinned (Installed by apt with no version: fetched/03-README.md line 39 ('sudo apt-get install mysql-server').)	—
spectral-workbench.js (core spectral JavaScript library)	not determined	not determined (Included from https://github.com/publiclab/spectral-workbench.js with no pinned revision; no manifest for it was fetched this run.)	—

Component	Finding	Severity	Fix available?
Bundler 1.17.2	The Bundler version recorded in the lockfile can be tricked into installing code from an attacker-controlled gem source when dependencies are installed. — GHSA-jvgm-pfqv-887x , GHSA-fp4w-jxhp-m23p , GHSA-g98m-96g9-wfjq , GHSA-fj7f-vq84-fh43	critical	Yes — update to 2.2.33 or later; Bundler is installed by the person setting the machine up, not pinned by the project.
Nokogiri 1.13.8	Nokogiri, which parses the XML and HTML the application handles, is 20 advisories behind including critical flaws in the libxml2 library it bundles. — GHSA-353f-x4gh-cqq8 , GHSA-qv4q-mr5r-qprj , GHSA-mrxw-mxhj-p664	critical	Yes — update to 1.18.9, allowed by the lockfile's 'nokogiri (~> 1.8)' requirement; confirm it installs on Ruby 2.6.6 before relying on it.
Puma 5.6.4	The web server students connect to has a critical HTTP request-smuggling flaw, which matters only if the server is ever reachable from beyond the host machine. — GHSA-68xg-gqqm-vgj8 , GHSA-c2f4-cvqm-65w2 , GHSA-9hf4-67fc-4vf4	critical	Yes — update to 5.6.9; the Gemfile declares 'gem "puma"' with no version constraint, so nothing blocks it.
Ruby on Rails (activerecord, activestorage) 5.2.4.6	The pinned Rails 5.2.4.6 carries critical remote-code-execution and arbitrary-file-read advisories in Active Record and Active Storage, both of which handle the spectrum images students upload. — GHSA-3hbc-qp5v-9p2j , GHSA-w749-p3v6-hccq , GHSA-r4mg-4433-c7g3 , GHSA-xr9x-r78c-5hrm (+1 more)	critical	No — project pins rails ~> 5.2.4.3, which excludes the fixed 5.2.6.3 and 5.2.8.1 releases; upgrading means editing the Gemfile.

Component	Finding	Severity	Fix available?
Rack 2.2.4	Rack, the layer every HTTP request passes through, is 30 advisories behind, including directory traversal and several memory-exhaustion denial-of-service issues. — GHSA-mxw3-3hh2-x2mh , GHSA-h2jq-g4cq-5ppq , GHSA-8vqr-qjwx-82mw , GHSA-v569-hp3g-36wr (+2 more)	high	Yes — update to 2.2.23, which satisfies the lockfile's own 'rack (~> 2.0, >= 2.0.8)' requirement.
rails-html-sanitizer 1.4.3 / loofah 2.18.0	The libraries that strip dangerous markup out of user-submitted text have cross-site-scripting and uncontrolled-recursion flaws, which is what a student comment or spectrum title would flow through. — GHSA-5x79-w82f-gw8w , GHSA-9h9g-93gc-623h , GHSA-mcvf-2q2m-x72m , GHSA-rrfc-7g8p-99q8 (+3 more)	high	Yes — update to rails-html-sanitizer 1.4.4 and loofah 2.19.1, both allowed by the lockfile's '~> 1.0' and '~> 2.3' requirements.
REXML 3.2.5	The bundled XML parser can be locked up by a malformed document, stalling the server. — GHSA-vmwr-mc7x-5vc3 , GHSA-2rxp-v6pw-ch6m , GHSA-5866-49gr-22v4 , GHSA-r55c-59qm-vjw6 (+2 more)	high	Yes — update to 3.3.9, allowed by the lockfile's 'rexml (>= 3.2.5, < 4.0)' requirement.
Ruby on Rails (actionpack, actionview, actionmailer, activerecord) 5.2.4.6	The same Rails 5.2.4.6 stack carries information-exposure and cross-site-scripting advisories in the request, view and mail layers that a student's browser session would be exposed to. — GHSA-wh98-p28r-vrc9 , GHSA-mm33-5vfq-3mm3 , GHSA-ch3h-j2vf-95pv , GHSA-cr5q-6q9f-rq6q (+2 more)	high	No — project pins rails ~> 5.2.4.3, which excludes the fixed 5.2.6.2 and 5.2.7.1 releases.
Transitive gems: addressable 2.8.0, concurrent-ruby 1.1.10, websocket-driver 0.7.5, mail 2.7.1, globalid 1.0.0, msgpack 1.5.4	Six supporting libraries carry denial-of-service, memory-exhaustion and email-spoofing advisories; none is pinned directly by the project, so all can move. — GHSA-h27x-rffw-24p4 , GHSA-h8w8-99g7-qmvj , GHSA-2x63-gw47-w4mm , GHSA-33ph-fccm-39pj (+3 more)	high	Yes — update to addressable 2.9.0, concurrent-ruby 1.3.7, websocket-driver 0.8.2, mail 2.9.1, globalid 1.0.1 and msgpack 1.8.2.
rdiscount 2.2.0.2	The Markdown renderer reads past the end of a buffer on crafted input. — GHSA-6r34-94wq-jhrc	moderate	No — project pins rdiscount 2.2.0.2 exactly in the Gemfile; the fix is 2.2.7.4.

Component	Finding	Severity	Fix available?
RMagick 4.2.6	A memory leak in the image-processing binding used on every uploaded spectrum image; it degrades a long-running server rather than exposing data. — GHSA-frgf-8jr5-j2jv	moderate	Yes — update to 5.3.0; the Gemfile declares 'gem "rmagick"' with no version constraint.
Gemfile dependency constraints	Dependencies unpinned: 31 of 34 in the Gemfile — the lockfile does pin all 102 resolved gems, so an install that uses the lockfile is reproducible, but any 'bundle update' moves versions the project never fixed.	posture	Mitigation only — always install from the committed Gemfile.lock (bundle install --deployment) rather than resolving fresh.
Host operating system (Ubuntu 18.04 LTS)	Ubuntu 18.04's standard support ended 2023-05-31; it still receives security updates only under extended (ESM) maintenance, through 2028-04-26.	posture	Mitigation only — attach an Ubuntu Pro/ESM subscription so the machine still gets patches, or install on a current LTS release.
Ruby language runtime 2.6.6	The Ruby version the project requires reached end of life on 2022-03-31, so the runtime under the whole application receives no security fixes at all.	posture	No — requires platform migration; moving off Ruby 2.6 means upgrading Rails, which the Gemfile's rails ~> 5.2.4.3 pin also blocks.
Student login and hosted spectra (publiclab.org / spectralworkbench.org)	Logging in redirects students to publiclab.org to approve an OpenID identity, and the documented workflow publishes spectra to the public spectralworkbench.org service — so student accounts and their uploaded data leave the campus network to third-party hosts.	posture	Mitigation only — decide in advance whether students use personal Public Lab accounts and whether spectra are published publicly; a purely local instance still requires the publiclab.org redirect to log in.

What this means for your lab

This spectrometer's hardware is just a USB webcam — it has no network connection of its own and nothing to attack. The risk lives entirely in the Spectral Workbench software students run on the host computer. That software is frozen on a 2022-era stack: Ruby 2.6.6 stopped receiving security fixes in March 2022, and the Rails version the project pins carries flaws that would let someone who can reach the server run their own code on that machine and read files off it. The project's own version pin blocks the Rails fix, so this is not something an instructor can simply patch away. Practically: run it on a machine that is not reachable from the campus network or the internet — the documented workflow is a local server at localhost:

3000, and it should stay that way. Do not expose it on a shared lab network, and do not put anything sensitive on that host. A few pieces can be updated safely (the Puma web server, Rack, Nokogiri, the HTML sanitisers, and Bundler itself), and doing so is worthwhile, but it does not fix the underlying end-of-life runtime. Separately, be aware that logging in sends students to publiclab.org to approve an account, and the documented workflow publishes spectra to the public spectralworkbench.org site — decide before class whether student names and data should go there, and raise this with campus IT before connecting the host to any network you do not control.

Not checked

- ImageMagick and its development headers (imagemagick, ruby-rmagick, libmagickwand-dev, libmagick++-dev): Installed by apt with no version constraint (fetched/03-README.md line 43); the installed version is whatever the host distribution ships, so there is no version to check.
- Node.js, npm and Yarn: Installed with no version constraint (fetched/03-README.md lines 64-72); nothing pins a version to check.
- Database engine (MySQL Server or SQLite3): Installed by apt with no version constraint (fetched/03-README.md line 39); the version is set by the host distribution.
- spectral-workbench.js (core spectral JavaScript library): Included from its own repository with no pinned revision; no manifest or lockfile for it was fetched this run, so no version exists to check.
- Debian/Ubuntu system packages generally: The lab's install instructions use apt without versions, so their advisory status depends on the host's own patch level rather than on anything the project records.
- publiclab.org and spectralworkbench.org hosted services: Neither host's pages could be downloaded by the checker this run, so their current availability and configuration were not established.
- Remaining 82 pinned gems in Gemfile.lock: Checked against OSV and clean at their pinned versions; listed here only to note that a clean result reflects today's advisory data, not a guarantee.

Parts

Part	Spec/Package	Status	Stock	Price	Source
Focus-Adjustable USB Webcam Module	UVC USB 2.0 camera module, 5 V bus, ≤ 500 mA, manual focus at 200 mm	readily available	in stock, multiple sellers	~~\$16.00~~ – ~~\$48.30~~	eBay (ELP mini UVC module); svpro.cc (ELP manual-focus model)

Part	Spec/Package	Status	Stock	Price	Source
Transmission Diffraction Grating	Linear transmission grating, 800–1350 lines/mm, ~20 mm × 20 mm	readily available	in stock, multiple sellers	\$2.15 - \$12.38	Home Science Tools; Bartovation 1,000 lines/mm; Arbor Scientific 5-pack \$6.00
Precision Slit Card (0.2 mm Aperture)	Cardstock insert ~35 mm × 35 mm, 0.2 mm slit	not checked	—	—	Template at publiclab.org/n/11246 — could not be downloaded this run
Spectrometer Enclosure Base (Bottom Chassis)	Cut sheet ~430.0 mm × 305.9 mm, matte black cardstock	readily available (cut file live)	—	not checked (cardstock/laser cutting not priced)	spec-box-bottom.svg — fetched successfully
Spectrometer Enclosure Lid and Angle Brackets	Cut sheet ~367.9 mm × 278.9 mm, 45° and 65° brackets	readily available (cut file live)	—	not checked (cardstock/laser cutting not priced)	spec-box-top+angles.svg — downloaded (pure vector, no text to extract)
Light-Blocking Assembly Tape	Opaque matte black tape, 12–25 mm wide	readily available	in stock, multiple sellers	\$9.79 - \$21.52	Walmart seller (blackout tape); Filmtools (Shurtape P743 matte black); \$12.00 CP-743, 1/2" at M. Cramer & Associates
USB Interface Cable — Tensility 10-00648	Shielded USB 2.0 cable assembly, ≥ 1 m	readily available (Active)	123	\$3.51	DigiKey (Tensility International Corp)

Notes on two rows above. The webcam: the fetched ELP-USB100W03M product page confirms UVC ("Free Drive Protocol: USB Video Class(UVC)"), DC5V USB bus power at 100–120 mA — comfortably inside the ≤ 500 mA budget — an OV9712 visible-light CMOS sensor, a 38 × 38 mm board (32 × 32 mm compatible) and a standard 1 m cable. It does not state manual focus. The one fetched page that does state manual focus (the ELP CS 2.8–12mm model, \$46.20) carries it in the product title only; its spec table did not extract, so its board size and UVC status are not evidence. The grating: the 1,000 lines/mm figure comes from the seller's listing title — the fetched Bartovation page confirms the construction ("highly efficient embossed Holographic Optical Elements ... used for the direct viewing and analysis of spectra") but its variant table did not extract.

The USB cable is often not a separate purchase at all: the snapshot notes the cable is typically captive on the webcam module, and the fetched ELP page lists a 1 m cable as included.

Substitutes

None needed. No part in this bill of materials is obsolete, out of stock, unobtainable, or overpriced, so no substitute was proposed or verified. The alternatives the lab itself documents — a peeled DVD-R data layer in place of a purchased grating, 3D-printed 45°/65° brackets in place of the cardstock ones, any opaque substrate for the slit card — are design latitude the snapshot already grants, not substitutions this check needed to make.

Verify any substitute against its datasheet before ordering.

Other dependencies

- **Enclosure cut files on GitHub** — LIVE. `spec-box-bottom.svg` fetched successfully from github.com/publiclab/spectrometer3; `spec-box-top+angles.svg` downloaded as well (pure vector art, so no text came back — the download itself is what confirms it is still served). The repository page also responded, returning its description "Public Lab's open source Desktop Spectrometry Kit"; its file listing is JavaScript-rendered and did not extract, so the two files were confirmed individually instead.
- **publiclab.org research notes and wiki pages** — NOT CHECKED. The lab depends on a large body of documentation there: lens focusing (/n/7226), grating angle (/n/5964, /n/5892), the removable slit card (/n/11246), calibration (/n/191), linearity (/n/10476, /n/6225), the hardware wikis (/wiki/dsk, /wiki/spectrometer) and the application notes (/n/174, /n/10015, /n/10955, /n/10382, /n/10012, /n/9432, /n/6168, /n/7475, /n/4406, /n/8995). Two representative URLs were fetched and both came back "Page could not be downloaded (blocked, timeout, or gone)"; the rest were not individually attempted. Check them in a browser before the term starts and keep local copies of anything students need.
- **Fabrication** — base sheet 430.0 mm × 305.9 mm and lid sheet 367.9 mm × 278.9 mm, cut and fold layers on separate vector layers, matte black interior finish, 80–100 lb cardstock or thin e-flute board. Taken from the snapshot; nothing external to check.
- **Laser cutter or craft cutting plotter access, and the cardstock itself** — not checked. No pricing was gathered for the raw substrate or for a cutting service.

Watch list

- **publiclab.org documentation** — the biggest risk to this lab by the next check. The parts are commodities; the irreplaceable asset is the community's calibration, alignment and application notes. Nothing in this run could confirm they are reachable. If that site goes away, the hardware is still buildable but the pedagogy around it is not.
- **The webcam** — a generic COTS line item with no stable part number. Specific models churn constantly, and "manual focus" quietly disappears from listings as vendors move to fixed-focus and autofocus modules. Expect to re-select a model, not re-order one.

- **The GitHub cut files** — live today, but the repository is the single point of failure for the enclosure. Mirror `spec-box-bottom.svg` and `spec-box-top+angles.svg` locally now.
- **The Spectral Workbench software stack** — see the Cybersecurity section above; it is the part of this lab that has actually drifted, and it will keep drifting.