

Readiness report — MagicMirror Smart Display

Checked 2026-09-03 18:30 · 8 searches, 3 pages fetched

Readiness: MagicMirror Smart Display

Verdict: Ready with caveats · 2026-09-03 · est. parts cost \$130-\$235, excluding the custom-cut two-way mirror **Cybersecurity — software & network: Review before networking**

Every part this lab needs is a current, in-stock consumer item available from several sellers today — there is nothing obsolete, back-ordered or single-sourced in the whole bill of materials, and no PCB to fabricate. Two things stop this being a clean "Ready". The two-way mirror, the one part specific to this build, is cut to order and the supplier publishes no prices, so that line has no cost on the record. And the lab specifies neither the display size nor the Raspberry Pi's RAM, so the two biggest cost drivers are left to the instructor and the total cannot be bounded from the BOM. This is the cold check for this lab: it establishes the baseline, and every price and stock position below is recorded so the next run can measure drift against it.

Action required

None — all checked parts are sourceable.

Cybersecurity — software & network

Review before networking — The network-facing WebSocket parser and web server carry fixable known flaws and the documented remote-access mode is unauthenticated, so the build is fine on a bench but should be patched and segmented before it goes on a shared network.

Component	Version	How known	Support status
MagicMirror ²	2.37.0	read from project (version field of fetched/01-package.json (tag v2.37.0); also pinned as magicmirror@2.37.0 in fetched/02-package-lock.json)	—
Node.js	22.21.1	inferred (lower bound of the engines.node range '>=22.21.1 <23 >=24' in fetched/01-package.json; the range is not a pin, so the installed version depends on what the instructor installs)	supported until 2027-04-30
Raspberry Pi OS	not determined	unpinned (docs_requirements.md says 'latest full version with Desktop'; no numeric release or codename is stated anywhere in the lab materials)	—

Component	Version	How known	Support status
Electron	42.5.2	read from project (fetched/02-package-lock.json (root optionalDependency; package.json declares the range ^42.5.2))	—
express	5.2.1	read from project (fetched/02-package-lock.json (the HTTP server behind port 8080))	—
socket.io	4.8.3	read from project (fetched/02-package-lock.json (the WebSocket server on port 8080))	—
socket.io-parser	4.2.6	read from project (fetched/02-package-lock.json (transitive via socket.io 4.8.3, declared range ~4.2.4))	—
undici	8.5.0	read from project (fetched/02-package-lock.json at node_modules/undici (root dependency, declared ^8.5.0) - the HTTP client used for weather, news and calendar fetches)	—
undici (build/test copy)	7.28.0	read from project (fetched/02-package-lock.json at node_modules/@electron/get/node_modules/undici and node_modules/jsdom/node_modules/undici)	—
qs	6.15.3	read from project (fetched/02-package-lock.json (transitive via express 5.2.1 ^6.14.0 and body-parser 2.3.0 ^6.15.2))	—
deepmerge-ts	7.1.5	read from project (fetched/02-package-lock.json (transitive via html-to-text 10.0.0, declared range ^7.1.5))	—
brace-expansion	5.0.7	read from project (fetched/02-package-lock.json (transitive via minimatch 10.2.5, declared range ^5.0.5; lint and test tooling only))	—
helmet	8.2.0	read from project (fetched/02-package-lock.json (HTTP security headers middleware); checked against OSV with no advisories)	—
express-basic-auth	1.2.1	read from project (fetched/02-package-lock.json (the optional HTTP authentication the snapshot describes); checked against OSV with no advisories)	—
node-ical	0.26.1	read from project (fetched/02-package-lock.json (fetches remote iCalendar files); checked against OSV with no advisories)	—
feedme	2.0.2	read from project (fetched/02-package-lock.json (parses remote RSS/Atom feeds); checked against OSV with no advisories)	—
html-to-text	10.0.0	read from project (fetched/02-package-lock.json (renders remote feed HTML to text))	—

Component	Version	How known	Support status
MagicMirrorOS (alternative image)	not determined	not determined (docs_installation.md names https://github.com/guysoft/MagicMirrorOS but states no version)	—
MagicMirror Docker image (alternative)	not determined	not determined (docs_installation.md names https://gitlab.com/khassel/magicmirror but states no version or tag)	—
MagicMirror Kubernetes Helm chart (alternative)	not determined	not determined (docs_installation.md names https://gitlab.com/khassel/magicmirror-helm but states no chart version)	—

Component	Finding	Severity	Fix available?
brace-expansion	Two denial-of-service flaws in a file-matching helper used by the project's lint and test tooling; the running mirror does not reach this code. — GHSA-rgw5-rvv9-x895 , GHSA-mh99-v99m-4gvq	high	Yes — update to 5.0.9
deepmerge-ts	The helper that merges options for the HTML-to-text converter, which processes remote RSS and calendar content, can exhaust the stack on a deeply nested document and crash the mirror. — GHSA-ggr8-5vv4-36mx	high	No — project pins ^7.1.5 via html-to-text 10.0.0, and the fix is in 8.0.0
socket.io-parser	The parser that reads WebSocket messages arriving on the mirror's port 8080 can be driven out of memory by a client sending specially shaped packets, which takes the display offline until it is restarted. — GHSA-2m8v-j782-fhvr	high	Yes — update to 4.2.7
undici	The HTTP client the mirror uses to pull weather, news feeds and calendars mishandles caching and cookie headers, so a hostile or compromised feed server can crash the fetch or cause one response to be served in place of another. — GHSA-4cwx-7wf7-3272 , GHSA-jr45-8vmc-qm54 , GHSA-8xcm-r25x-g524 , GHSA-v3r7-h72x-cjcm (+1 more)	high	Yes — update to 8.9.0
undici (build/test copy)	A second, older copy of the same HTTP client is installed under the Electron downloader and the test browser, so it is reached only when building or testing the project, not by the running mirror. — GHSA-4cwx-7wf7-3272 , GHSA-jr45-8vmc-qm54 , GHSA-8xcm-r25x-g524 , GHSA-v3r7-h72x-cjcm (+1 more)	high	Yes — update to 7.29.0

Component	Finding	Severity	Fix available?
qs	The query-string parser inside the mirror's web server can be made to consume excessive CPU, or to slip past its own array-size limit, by a crafted request to port 8080. — GHSA-4mjr-xmp4-gh2g , GHSA-x5fp-wj9c-mxmx	moderate	Yes — update to 6.16.0
MagicMirror ²	All 45 dependencies in the project's package.json are declared as caret ranges and the copy uploaded for this lab ships no lockfile, so two instructors installing on different days get different code; the versions checked above are upstream's package-lock.json for tag v2.37.0, not necessarily what will land on the mirror.	posture	Mitigation only — install with upstream's v2.37.0 package-lock.json using 'npm ci' rather than 'npm install', so the versions checked here are the versions deployed
MagicMirror ²	The application ships no username or password, and the documented way to reach it from another machine is to bind it to 0.0.0.0 and widen the ipWhitelist, at which point anything the whitelist admits can read the dashboard and open a WebSocket to it with no login.	posture	Mitigation only — keep the default localhost binding where possible; if remote access is needed, keep ipWhitelist to specific addresses and turn on the optional express-basic-auth
Raspberry Pi OS	The lab installs whatever Raspberry Pi OS Desktop release is current rather than a recorded one, so the operating system underneath a network-facing service has no version anyone can check for patches or end-of-life.	posture	Mitigation only — record the Raspberry Pi OS release written to the card and run a full system update before the lab is used

What this means for your lab

Out of the box this mirror is fairly contained: it only listens on its own machine, so nobody else on the network can reach it, and it has no default password to leak. The risk starts the moment you follow the documentation's instructions for viewing the mirror from another computer, because that opens the dashboard to the network with no login at all - anyone the address filter lets through can read whatever the mirror displays, which usually means your calendar, your location's weather and any feeds you added. On top of that, the WebSocket parser and the web server's query handling both have known flaws that let a visitor on the network crash the display, and the component that fetches your calendars and news feeds can be tripped up by a hostile feed. Most of these have updates available; one, in the HTML-to-text converter, does not and cannot be fixed without the project moving to a newer version of that library. Two other things are simply unknown rather than safe: the lab installs whatever Raspberry Pi OS release is current instead of a recorded one, and it ships no lockfile, so the exact software you end up running is not the software checked here. Practically: keep the mirror on a staff or IoT network segment rather than the open campus network, do not enable

remote viewing unless you also turn on the optional password protection, run a full system update before class, and let campus IT know it is there before you plug it in.

Not checked

- Raspberry Pi OS: Installed as 'latest full version with Desktop'; no numeric release or codename is stated, so no end-of-life or advisory lookup was possible.
- 173 transitive npm dependencies from package-lock.json: Beyond this run's 500-row automatic OSV check cap (676 pinned rows in the lockfile, 500 checked).
- MagicMirrorOS (guysoft/MagicMirrorOS): Alternative install image; the lab's documentation states no version, so there was nothing to look up.
- MagicMirror Docker image (khassel/magicmirror): Alternative install path; the lab's documentation states no image tag or version.
- MagicMirror Kubernetes Helm chart (khassel/magicmirror-helm): Alternative install path; the lab's documentation states no chart version.
- Third-party MagicMirror modules and community scripts (sdetweil/MagicMirror_scripts, Bee-Mar/mmpm): Named in the lab's external links but carry no version or check plan in the snapshot; whatever an instructor installs from them is unchecked code.
- Electron 42.5.2: Checked against OSV with no advisories, but Electron bundles a Chromium build whose own patch level is not visible from the lockfile and was not checked separately.
- 173 further dependencies in package-lock.json: beyond the 500-dependency automatic check cap (e.g. istanbul-lib-report, istanbul-reports, js-tokens, jsdoc-type-pratt-parser, jsonc-eslint-parser)

Parts

Part	Spec/Package	Status	Stock	Price	Source
Host single-board computer	Raspberry Pi 4 Model B, 85 × 56 mm, 5 V ≥3.0 A USB-C	Readily available	In stock, multiple sellers	\$35.00 – \$165.00 by RAM	CanaKit, PiShop USA, Mouser, eBay
Host power supply adapter	100–240 V AC in, 5.1 V DC out, 3.0 A (Pi 4) / 5.0 A (Pi 5), USB-C	Readily available	In stock, six sellers	\$8.00 (Pi 4) / \$14.04 (27 W, 5.1 V 5 A)	DigiKey, Adafruit
MicroSD flash storage card	32 GB, Class 10, UHS-I, microSDHC	Readily available	In stock	\$20.99	Walmart (First Choice Online)
HDMI video interconnect cable	Micro-HDMI (type D) male to full-size HDMI male, 1 m	Readily available	In stock, four sellers	\$3.26 – \$6.95	Computer Cable Store, PiShop USA

Part	Spec/Package	Status	Stock	Price	Source
Computer monitor / flat-panel display	Any HDMI-input panel; thin bezel preferred for mirror mounting	Readily available	In stock, seven sellers	~~\$69.19~~ – \$119.99	Walmart (Gawfolk 22" bezel-less)
Two-way semi-transparent mirror	70% reflective / 30% transparent, glass or acrylic, cut to panel size	Readily available (not priced)	Ships immediately; 1-day cutting for sizes up to 63" × 96"	Quote required — supplier publishes no prices	twowaymirrors.com (Toledo, OH)
Computer keyboard	Standard USB keyboard, 5 V bus powered	Readily available	In stock, seven sellers	~~\$11.99~~ – ~~\$14.99~~	Best Buy, Dell

Three wrong-variant listings to avoid. All three sit inside otherwise healthy search results for the parts above:

- The Micro Center "Raspberry Pi White Mini HDMI to HDMI" at \$3.99 is **mini** HDMI (type C), not **micro** HDMI (type D). It will not mate with a Pi 4 or Pi 5.
- The eBay "SanDisk Ultra SDHC SDCSDUNC-032G-AN6IN" at \$20.00 is a **full-size SD card**, not microSD.
- The 32 GB microSD listings at \$53.99, \$54.99 and \$68.79 are phone-accessory bundles — the same class of card at 2.5–3.3× the \$20.99 price.

Substitutes

None needed.

Other dependencies

- **Fabrication: none required.** The snapshot records no PCBs, Gerber files, drill data or layer stackups — the build is entirely off-the-shelf hardware plus cut optical glass.
- **Two-way mirror supplier** — <https://www.twowaymirrors.com/smart-mirror/> is live and was fetched this run. It states 70% reflective / 30% transparent stock in glass or acrylic, 5 mm glass, a maximum size of 96" × 126", cutting accuracy $\pm 1/16$ ", immediate shipping and a one-day cutting lead time for sizes up to 63" × 96" (tempering adds about a week). It publishes no prices; sizes are quoted individually.
- **Upstream Git repository** — <https://github.com/MagicMirrorOrg/MagicMirror.git> was reachable this run; the project's files at release tag v2.37.0 were fetched successfully.
- **Project website** <https://magicmirror.builders> — not checked.
- **Documentation site** <https://docs.magicmirror.builders> — not checked.
- **Community support forum** <https://forum.magicmirror.builders> — not checked.

- **Original project blog** <https://michaelteeuw.nl/tagged/magicmirror> — not checked.

Watch list

- **The two-way mirror is the only unpriced line and the only made-to-order part.** Get a written quote for your chosen panel size before committing a budget — it is the largest unknown in the build and cannot be substituted from a shelf.
- **Raspberry Pi pricing swings with RAM and channel.** The same board ranged from \$35.00 to \$165.00 this run, and the distributor listing was roughly 1.8× the marketplace price for 8 GB. Decide the RAM you actually need before ordering; the lab does not specify one.
- **Pi generation drives two other lines.** A Pi 2 or 3 needs a full-size HDMI cable and a micro-USB supply rather than the micro-HDMI cable and USB-C supply priced here; only the Pi 4 path was checked.
- **Monitor availability is by model, not by category.** The specific panels priced here are consumer stock that rotates; the category will stay cheap and plentiful, but expect these exact models to be gone by the next check.
- **The \$8.00 official Pi 4 power supply is the cheapest correct part but its amperage is not stated in the listing.** Confirm it is the 15 W / 3 A official unit before buying for a Pi 4, and note a Pi 5 needs the 27 W / 5 A version instead.