VulnBeacon

Regulation (EU) 2024/2847: Cyber Resilience Act: readiness report

Platform Worker Image 2026.07.06 · Generated 2026-11-01 22:35 UTC · Evidence as of 2026-11-01 22:33 UTC

Regulation (EU) 2024/2847 of 23 October 2024, OJ L of 20 November 2024. The Art. 14 reporting obligations apply from 11 September 2026 and the rest of the Regulation from 11 December 2027 (Art. 71).

Essential requirements for products with digital elements: selected Annex I Part I product properties, the Part II vulnerability-handling requirements (1) to (8), the Art. 13(8) support period and the Art. 14 reporting obligations.

34.4%
readiness

● Blocked

Do not present this product as ready until the blocking gaps are closed or formally justified.

Across 16 applicable controls: 4 satisfied · 3 needs attention · 4 gap · 5 awaiting attestation

- 3 active findings are past SLA.
- The release policy gate is failing.
- 4 framework controls are in gap state.

Executive summary

Decision	Active findings	SLA exposure
Blocked	**26**	**3 overdue**
3 active findings are past SLA.	0 KEV, 24 fixable	0 at risk

Inventory	Release gate	VEX coverage
67%	**Gate failed**	**0.0%**
2 generations, 13d	2 audit events in 90d	0/2 fixless documented

What changed

No previous readiness snapshot is available yet; this report is the baseline.

Daily snapshots will show improvement/regression history after the next run.

Product scope

Product	Platform Worker Image
Version	2026.07.06
Business owner	Platform Operations
Account owner	example account
Environment	production
Criticality	high
Customer-facing	No
Internet-facing	No

Top business actions

Prioritised actions convert control gaps into product-owner work.

Priority	Citation	Business action	Status
Critical Unblock release	`Annex I Part I (2)(a)`	**Made available without known exploitable vulnerabilities** Policy gate failing: Malicious packages (2) exceeds the limit of 0: eslint-plugin-restart-vega-soap@1.0.0, py-infopullhydra@1.0.0 Enforce a release gate: the org policy gate must be configured and the latest assessment must pass (no KEV/critical findings above threshold) before shipping.	● Gap

Priority	Citation	Business action	Status
Critical Unblock release	`Annex I Part II (2)`	**Address and remediate vulnerabilities without delay** 26 active findings: 3 overdue, 0 at risk (≤14d); SLA budgets: KEV: CISA due date, critical 5d, high 21d, medium 60d, low 120d, at-risk window 7d. No active finding should exceed its SLA due date (KEV due dates from CISA, severity budgets from the org policy).	Gap
High Complete audit evidence	`Annex I Part II (4)`	**Publicly disclose information about fixed vulnerabilities** Requires manual evidence. Attest below with a note or URL. Publish security advisories for fixed vulnerabilities (the product advisory export produces the artifact); attest with the URL of your advisory feed or page.	Awaiting attestation
High Complete audit evidence	`Annex I Part II (5)`	**Coordinated vulnerability disclosure policy in place** Requires manual evidence. Attest below with a note or URL. Publish a CVD policy (e.g. security.txt + policy page) covering intake, triage timelines, and safe-harbor; attest with its URL.	Awaiting attestation
High Complete audit evidence	`Annex I Part II (6)`	**Contact address for reporting vulnerabilities** Requires manual evidence. Attest below with a note or URL. Provide and monitor a security contact (security@ mailbox or intake form); attest with the address/URL.	Awaiting attestation

Priority	Citation	Business action	Status
High Complete audit evidence	`Annex I Part II (7)`	**Secure distribution mechanism for updates** Requires manual evidence. Attest below with a note or URL. Updates must be distributed via a mechanism that ensures integrity and authenticity (signed packages/attested pipeline); attest with a short description or documentation link.	Awaiting attestation
High Complete audit evidence	`Art. 14(1) to (4)`	**Actively exploited vulnerabilities and severe incidents notified through the single reporting platform** Requires manual evidence. Attest below with a note or URL. Art. 14: an actively exploited vulnerability in the product is notified to the coordinator CSIRT and ENISA through the single reporting platform with an early warning within 24…	Awaiting attestation
Medium Improve evidence quality	`Annex I Part II (1)`	**SBOM covers at least the top-level dependencies, machine-readable** NTIA-element coverage 67% (grade C): 10/10 versioned, 10 with PURL/CPE, 0 with supplier, 0 with hash digests. Raise NTIA-minimum-element coverage: component versions, identifiers (PURL/CPE), and suppliers.	Needs attention

Evidence inventory

Business, audit, and customer hand-off evidence available for this product.

Evidence area	Current evidence	State
Latest product inventory	Latest SBOM (trivy); 10 components; uploaded 2026-10-19T10:37:58Z; release 2026.07.06; sha256 242ec7b611e1ee8a	Satisfied
Inventory quality	NTIA-element coverage 67% (grade C).	Needs attention
Vulnerability response	3 active findings are overdue against the SLA policy.	Gap
Exploited vulnerability handling	No active CISA KEV findings.	Satisfied
Remediation plan	24 fixable findings; plan covers 6 components.	Satisfied
VEX and disposition coverage	0/2 fixless findings documented (0.0%).	Gap
Continuous monitoring	Vulnerability data refreshed automatically: no; 13 snapshots in the last 30 days.	Needs attention
Alert routing	0 active external destinations; in-app alerts remain enabled.	Needs attention
Audit trail	2 product-scoped audit events in the last 90 days.	Satisfied
Machine-readable hand-off artifacts	Evidence pack, VDR, CSAF VEX, OpenVEX, and advisory exports are available. Evidence pack · CycloneDX VDR · CSAF VEX · OpenVEX · Advisory	Satisfied
Owner attestations	5 pending, 0 marked not applicable.	Needs attention

Framework control matrix

Each citation links to its entry under Framework text, which carries the requirement's full guidance and where the cited text is published.

Product security properties

Citation	Control and evidence	Status	Next step
Annex I Part I (2)(a)	**Made available without known exploitable vulnerabilities** Policy gate failing: Malicious packages (2) exceeds the limit of 0: eslint-plugin-restart-vega-soap@1.0.0, py-infopullhydra@1.0.0	Gap	Enforce a release gate: the org policy gate must be configured and the latest assessment must pass (no KEV/critical findings above threshold) before shipping.
Annex I Part I (2)(c)	**Vulnerabilities addressed through security updates** MEDIUM: MTTR 6d, on-time 100.0% (SLA 60d, n=72); CRITICAL: MTTR 5d, on-time 60.0% (SLA 5d, n=10); HIGH: MTTR 7d, on-time 100.0% (SLA 21d, n=66); LOW: MTTR 7d, on-time 100.0% (SLA 120d, n=10)	Satisfied	—

Vulnerability handling

Citation	Control and evidence	Status	Next step
Annex I Part II (1)	**Identify and document components (SBOM)** SBOM (trivy), 10 components, uploaded 2026-10-19 (13d ago), sha256 242ec7b611e1ee8a…	Satisfied	—

Citation	Control and evidence	Status	Next step
Annex I Part II (1)	**SBOM covers at least the top-level dependencies, machine-readable** NTIA-element coverage 67% (grade C): 10/10 versioned, 10 with PURL/CPE, 0 with supplier, 0 with hash digests.	Needs attention	Raise NTIA-minimum-element coverage: component versions, identifiers (PURL/CPE), and suppliers.
Annex I Part II (2)	**Address and remediate vulnerabilities without delay** 26 active findings: 3 overdue, 0 at risk (≤14d); SLA budgets: KEV: CISA due date, critical 5d, high 21d, medium 60d, low 120d, at-risk window 7d.	Gap	No active finding should exceed its SLA due date (KEV due dates from CISA, severity budgets from the org policy).
Annex I Part II (2)	**Actively exploited vulnerabilities prioritised** No findings in the CISA KEV catalog.	Satisfied	—
Annex I Part II (2)	**Remediation path identified for fixable findings** 24 fixable findings, upgrade plan covers 6 components; 2 findings have no published fix yet.	Satisfied	—
Annex I Part II (3)	**Effective and regular tests and reviews of product security** Vulnerability data refreshed automatically: no; 13 nightly assessment snapshots in the last 30 days.	Needs attention	Continuous re-matching of the SBOM against fresh vulnerability data (nightly rematch + auto-sync) evidences regular review; complement with periodic penetration testing (attach as...

Citation	Control and evidence	Status	Next step
Annex I Part II (4)	**Publicly disclose information about fixed vulnerabilities** Requires manual evidence. Attest below with a note or URL.	Awaiting attestation	Publish security advisories for fixed vulnerabilities (the product advisory export produces the artifact); attest with the URL of your advisory feed or page.
Annex I Part II (5)	**Coordinated vulnerability disclosure policy in place** Requires manual evidence. Attest below with a note or URL.	Awaiting attestation	Publish a CVD policy (e.g. security.txt + policy page) covering intake, triage timelines, and safe-harbor; attest with its URL.
Annex I Part II (6)	**Contact address for reporting vulnerabilities** Requires manual evidence. Attest below with a note or URL.	Awaiting attestation	Provide and monitor a security contact (security@ mailbox or intake form); attest with the address/URL.

Updates

Citation	Control and evidence	Status	Next step
Annex I Part II (7)	**Secure distribution mechanism for updates** Requires manual evidence. Attest below with a note or URL.	Awaiting attestation	Updates must be distributed via a mechanism that ensures integrity and authenticity (signed packages/attested pipeline); attest with a short description or documentation link.

Citation	Control and evidence	Status	Next step
Annex I Part II (7)	**Build provenance attested for the update pipeline (integrity/authenticity)** No build-provenance attestation on file. Publish an in-toto/SLSA provenance attestation for the release (e.g. `cosign attest-blob` or a SLSA generator) and upload it under Release → Build provenance so the update pipeline's integrity and authenticity are evidenced.	Gap	An authenticated build pipeline is direct evidence of secure update distribution: publish an in-toto/SLSA provenance attestation for each release (e.g. `cosign attest-blob` or a...
Annex I Part II (8)	**Security patches disseminated without delay, with advisories** 0 active integration destinations (owner account); in-app alerts always on.	Needs attention	Alerting on new findings/fix availability plus a working advisory channel evidences timely dissemination; configure at least one alert destination.

Support period

Citation	Control and evidence	Status	Next step
Art. 13(8)	**Support period determined and declared (at least five years, unless the product is expected to be in use for less)** No support period declared on the product. Set its support end (and start) so the period is a documented decision and the vulnerability-handling controls are measured against it.	Gap	Art. 13(8): the manufacturer determines the support period so that it reflects the time the product is expected to be in use, and it is at least five years unless the product is...

Citation	Control and evidence	Status	Next step
`Art. 14(1) to (4)`	**Actively exploited vulnerabilities and severe incidents notified through the single reporting platform** Requires manual evidence. Attest below with a note or URL.	• Awaiting attestation	Art. 14: an actively exploited vulnerability in the product is notified to the coordinator CSIRT and ENISA through the single reporting platform with an early warning within 24...

Framework text

Regulation (EU) 2024/2847 of 23 October 2024, OJ L of 20 November 2024. The Art. 14 reporting obligations apply from 11 September 2026 and the rest of the Regulation from 11 December 2027 (Art. 71). Published text: https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

`Annex I Part I (2)(a)` · Made available without known exploitable vulnerabilities

Enforce a release gate: the org policy gate must be configured and the latest assessment must pass (no KEV/critical findings above threshold) before shipping.

Automated check over the product's data · Cited text

`Annex I Part I (2)(c)` · Vulnerabilities addressed through security updates

Demonstrate that findings are resolved within the org SLA. The report cites MTTR and on-time percentages per severity.

Automated check over the product's data · Cited text

`Annex I Part II (1)` · Identify and document components (SBOM)

Keep a machine-readable SBOM of the shipped release current. Re-upload on every release, because stale inventories undermine every downstream control.

Automated check over the product's data · Cited text

`Annex I Part II (1)` · SBOM covers at least the top-level dependencies, machine-readable

Raise NTIA-minimum-element coverage: component versions, identifiers (PURL/CPE), and suppliers. Re-export from your build tooling if fields are missing.

Automated check over the product's data · Cited text

Annex I Part II (2) · Address and remediate vulnerabilities without delay

No active finding should exceed its SLA due date (KEV due dates from CISA, severity budgets from the org policy).

Automated check over the product's data · Cited text

Annex I Part II (2) · Actively exploited vulnerabilities prioritised

Findings in the CISA KEV catalog must be remediated (or formally VEX-justified) before their CISA due dates.

Automated check over the product's data · Cited text

Annex I Part II (2) · Remediation path identified for fixable findings

Every fixable finding should have an identified upgrade target; use the Remediation tab's plan and file tickets from it.

Automated check over the product's data · Cited text

Annex I Part II (3) · Effective and regular tests and reviews of product security

Continuous re-matching of the SBOM against fresh vulnerability data (nightly rematch + auto-sync) evidences regular review; complement with periodic penetration testing (attach as manual evidence).

Automated check over the product's data · Cited text

Annex I Part II (4) · Publicly disclose information about fixed vulnerabilities

Publish security advisories for fixed vulnerabilities (the product advisory export produces the artifact); attest with the URL of your advisory feed or page.

Manual evidence required (owner attestation) · Cited text

Annex I Part II (5) · Coordinated vulnerability disclosure policy in place

Publish a CVD policy (e.g. security.txt + policy page) covering intake, triage timelines, and safe-harbor; attest with its URL.

Manual evidence required (owner attestation) · Cited text

Annex I Part II (6) · Contact address for reporting vulnerabilities

Provide and monitor a security contact (security@ mailbox or intake form); attest with the address/URL.

Manual evidence required (owner attestation) · Cited text

Annex I Part II (7) · Secure distribution mechanism for updates

Updates must be distributed via a mechanism that ensures integrity and authenticity (signed packages/attested pipeline); attest with a short description or documentation link.

Manual evidence required (owner attestation) · Cited text

`Annex I Part II (7)` · Build provenance attested for the update pipeline (integrity/authenticity)

An authenticated build pipeline is direct evidence of secure update distribution: publish an in-toto/SLSA provenance attestation for each release (e.g. `cosign attest-blob` or a SLSA generator), register a keyless (Fulcio identity) trust anchor, and upload the signed attestation so it is cryptographically verified and bound to the shipped SBOM. The reported SLSA level is a readiness estimate, not a conformance determination.

Automated check over the product's data · Cited text

`Annex I Part II (8)` · Security patches disseminated without delay, with advisories

Alerting on new findings/fix availability plus a working advisory channel evidences timely dissemination; configure at least one alert destination. The check proves the alerting half only: the advisory messages themselves are the Part II (4) disclosure control.

Automated check over the product's data · Cited text

`Art. 13(8)` · Support period determined and declared (at least five years, unless the product is expected to be in use for less)

Art. 13(8): the manufacturer determines the support period so that it reflects the time the product is expected to be in use, and it is at least five years unless the product is expected to be in use for a shorter time. Declare the period on the product (support start and end) so it is a documented decision and the vulnerability-handling controls are measured against it; state it in the information that accompanies the product (Annex II).

Automated check over the product's data · Cited text

`Art. 14(1) to (4)` · Actively exploited vulnerabilities and severe incidents notified through the single reporting platform

Art. 14: an actively exploited vulnerability in the product is notified to the coordinator CSIRT and ENISA through the single reporting platform with an early warning within 24 hours of becoming aware of it, a vulnerability notification within 72 hours and a final report within 14 days of a corrective or mitigating measure being available; a severe incident with an impact on the product's security follows 24 hours, 72 hours and one month. This obligation applies from 11 September 2026. Attest with the URL of the reporting procedure or of the record of the last notification.

Manual evidence required (owner attestation) · Cited text

This report is automated evidence and self-assessment input produced from the product's live vulnerability-management data (SBOM, findings, SLA state, VEX decisions, monitoring and audit activity) plus owner attestations. It supports a conformity assessment; it is not a certification. Machine-readable artifacts (CycloneDX VDR, CSAF VEX, OpenVEX) are available from the product's Export menu.

Generated by **VulnBeacon**