VulnBeacon

Règlement (UE) 2024/2847 : règlement sur la cyberrésilience : rapport de niveau de préparation

Platform Worker Image 2026.07.06 · Généré le 1 nov. 2026, 22:35 UTC · Preuves au 1 nov. 2026, 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).

Exigences essentielles pour les produits comportant des éléments numériques : une sélection des propriétés produit de l'annexe I partie I, les exigences de gestion des vulnérabilités (1) à (8) de la partie II, la période de support de l'art. 13(8) et les obligations de notification de l'art. 14.

34,4 %
niveau de préparation

● Bloqué

Ne présentez pas ce produit comme prêt tant que les écarts bloquants ne sont pas comblés ou formellement justifiés.

Sur 16 contrôles applicables : 4 satisfaits · 3 à surveiller · 4 écarts · 5 en attente d’attestation

- 3 constats actifs sont en dépassement de SLA.
- La barrière de publication est bloquée.
- 4 contrôles présentent un manque.

Synthèse

Décision	Constats actifs	Exposition SLA
Bloqué	**26**	**3 en retard**
3 constats actifs sont en dépassement de SLA.	0 KEV, 24 corrigeables	0 à risque

Inventaire	Barrière de publication	Couverture VEX
67 %	**Barrière en échec**	**0,0 %**
2 générations, 13 j	2 événements d’audit sur 90 j	0/2 sans correctif documentés

Ce qui a changé

Aucun instantané de préparation antérieur n’est encore disponible ; ce rapport sert de référence.

après le prochain passage.

Périmètre du produit

Produit	Platform Worker Image
Version	2026.07.06
Responsable métier	Platform Operations
Titulaire du compte	compte d’exemple
Environnement	production
Criticité	élevée
Exposé aux clients	Non
Exposé à Internet	Non

Principales actions métier

Les actions priorisées transforment les écarts de contrôle en travail pour le responsable du produit.

Priorité	Citation	Action métier	Statut
Critique Débloquer la publication	`Annex I Part I (2)(a)`	**Made available without known exploitable vulnerabilities** Barrière de publication en échec : 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.	● Écart

Priorité	Citation	Action métier	Statut
Critique Débloquer la publication	`Annex I Part II (2)`	**Address and remediate vulnerabilities without delay** 26 constats actifs : 3 en retard, 0 à risque (≤ 14 j) ; budgets SLA : KEV : échéance CISA, critique 5 j, élevée 21 j, moyenne 60 j, faible 120 j, fenêtre à risque 7 j. No active finding should exceed its SLA due date (KEV due dates from CISA, severity budgets from the org policy).	● Écart
Élevée Compléter les preuves d'audit	`Annex I Part II (4)`	**Publicly disclose information about fixed vulnerabilities** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL. Publish security advisories for fixed vulnerabilities (the product advisory export produces the artifact); attest with the URL of your advisory feed or page.	● En attente d'attestation
Élevée Compléter les preuves d'audit	`Annex I Part II (5)`	**Coordinated vulnerability disclosure policy in place** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL. Publish a CVD policy (e.g. security.txt + policy page) covering intake, triage timelines, and safe-harbor; attest with its URL.	● En attente d'attestation
Élevée Compléter les preuves d'audit	`Annex I Part II (6)`	**Contact address for reporting vulnerabilities** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL. Provide and monitor a security contact (security@ mailbox or intake form); attest with the address/URL.	● En attente d'attestation

Priorité	Citation	Action métier	Statut
Élevée Compléter les preuves d'audit	`Annex I Part II (7)`	**Secure distribution mechanism for updates** Preuve manuelle requise. Attestez ce contrôle avec une note ou une 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.	En attente d'attestation
Élevée Compléter les preuves d'audit	`Art. 14(1) to (4)`	**Actively exploited vulnerabilities and severe incidents notified through the single reporting platform** Preuve manuelle requise. Attestez ce contrôle avec une note ou une 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…	En attente d'attestation
Moyenne Améliorer la qualité des preuves	`Annex I Part II (1)`	**SBOM covers at least the top-level dependencies, machine-readable** Couverture des éléments NTIA 67 % (note C) : 10/10 versionnés, 10 avec PURL/CPE, 0 avec fournisseur, 0 avec empreintes. Raise NTIA-minimum-element coverage: component versions, identifiers (PURL/CPE), and suppliers.	À surveiller

Inventaire des preuves

Preuves métier, d'audit et de remise au client disponibles pour ce produit.

Domaine de preuve	Preuve actuelle	État
Dernier inventaire du produit	Dernier SBOM (trivy) ; 10 composants ; importé le 19 oct. 2026, 10:37 UTC ; version 2026.07.06 ; sha256 242ec7b611e1ee8a	Satisfait
Qualité de l'inventaire	Couverture des éléments NTIA 67 % (note C).	À surveiller
Réponse aux vulnérabilités	3 constats actifs en retard au regard de la politique SLA.	Écart
Traitement des vulnérabilités exploitées	Aucun constat KEV de la CISA actif.	Satisfait
Plan de remédiation	24 constats corrigeables ; le plan couvre 6 composants.	Satisfait
Couverture VEX et décisions	0/2 constats sans correctif documentés (0,0 %).	Écart
Surveillance continue	Données de vulnérabilité actualisées automatiquement : non ; 13 instantanés sur les 30 derniers jours.	À surveiller
Acheminement des alertes	0 destination externe active ; les alertes dans l'application restent actives.	À surveiller
Piste d'audit	2 événements d'audit propres au produit sur les 90 derniers jours.	Satisfait
Artefacts de remise lisibles par machine	Les exports dossier de preuves, VDR, CSAF VEX, OpenVEX et avis sont disponibles. Dossier de preuves · CycloneDX VDR · CSAF VEX · OpenVEX · Avis	Satisfait
Attestations du responsable	5 en attente, 0 marqué sans objet.	À surveiller

Matrice des contrôles du référentiel

Chaque citation renvoie à son entrée sous Texte du référentiel, qui reprend les indications complètes de l'exigence et l'endroit où le texte cité est publié.

Product security properties

Citation	Contrôle et preuve	Statut	Prochaine étape
`Annex I Part I (2)(a)`	**Made available without known exploitable vulnerabilities** Barrière de publication en échec : Malicious packages (2) exceeds the limit of 0: eslint-plugin-restart-vega-soap@1.0.0, py-infopullhydra@1.0.0	● Écart	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)	● Satisfait	—

Vulnerability handling

Citation	Contrôle et preuve	Statut	Prochaine étape
`Annex I Part II (1)`	**Identify and document components (SBOM)** SBOM (trivy), 10 composants, importé le 19 oct. 2026 (il y a 13 j), sha256 242ec7b611e1ee8a…	● Satisfait	—

Citation	Contrôle et preuve	Statut	Prochaine étape
Annex I Part II (1)	**SBOM covers at least the top-level dependencies, machine-readable** Couverture des éléments NTIA 67 % (note C) : 10/10 versionnés, 10 avec PURL/CPE, 0 avec fournisseur, 0 avec empreintes.	● À surveiller	Raise NTIA-minimum-element coverage: component versions, identifiers (PURL/CPE), and suppliers.
Annex I Part II (2)	**Address and remediate vulnerabilities without delay** 26 constats actifs : 3 en retard, 0 à risque (≤ 14 j) ; budgets SLA : KEV : échéance CISA, critique 5 j, élevée 21 j, moyenne 60 j, faible 120 j, fenêtre à risque 7 j.	● Écart	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** Aucun constat au catalogue KEV de la CISA.	● Satisfait	—
Annex I Part II (2)	**Remediation path identified for fixable findings** 24 constats corrigeables, le plan de mise à niveau couvre 6 composants ; 2 constats sans correctif publié à ce jour.	● Satisfait	—
Annex I Part II (3)	**Effective and regular tests and reviews of product security** Données de vulnérabilité actualisées automatiquement : non ; 13 instantanés d'évaluation nocturnes sur les 30 derniers jours.	● À surveiller	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	Contrôle et preuve	Statut	Prochaine étape
Annex I Part II (4)	**Publicly disclose information about fixed vulnerabilities** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL.	En attente d'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** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL.	En attente d'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** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL.	En attente d'attestation	Provide and monitor a security contact (security@ mailbox or intake form); attest with the address/URL.

Updates

Citation	Contrôle et preuve	Statut	Prochaine étape
Annex I Part II (7)	**Secure distribution mechanism for updates** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL.	En attente d'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	Contrôle et preuve	Statut	Prochaine étape
Annex I Part II (7)	**Build provenance attested for the update pipeline (integrity/authenticity)** Aucune attestation de provenance de build enregistrée. Publiez une attestation de provenance in-toto/SLSA pour la version (par exemple `cosign attest-blob` ou un générateur SLSA) et importez-la sous Publication → Provenance de build pour attester l'intégrité et l'authenticité de la chaîne de mise à jour.	● Écart	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 destination d'intégration active (compte du responsable) ; alertes dans l'application toujours actives.	● À surveiller	Alerting on new findings/fix availability plus a working advisory channel evidences timely dissemination; configure at least one alert destination.

Citation	Contrôle et preuve	Statut	Prochaine étape
Art. 13(8)	**Support period determined and declared (at least five years, unless the product is expected to be in use for less)** Aucune période de support déclarée sur le produit. Renseignez sa fin de support (et son début) pour que la période soit une décision documentée et que les contrôles de gestion des vulnérabilités s'y mesurent.	Écart	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…

Reporting obligations

Citation	Contrôle et preuve	Statut	Prochaine étape
Art. 14(1) to (4)	**Actively exploited vulnerabilities and severe incidents notified through the single reporting platform** Preuve manuelle requise. Attestez ce contrôle avec une note ou une URL.	En attente d'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…

Texte du référentiel

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). Texte publié : 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.

Vérification automatique sur les données du produit · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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).

Vérification automatique sur les données du produit · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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).

Vérification automatique sur les données du produit · Texte cité

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.

Preuve manuelle requise (attestation du responsable) · Texte cité

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.

Preuve manuelle requise (attestation du responsable) · Texte cité

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.

Preuve manuelle requise (attestation du responsable) · Texte cité

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.

Preuve manuelle requise (attestation du responsable) · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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.

Vérification automatique sur les données du produit · Texte cité

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).

Vérification automatique sur les données du produit · Texte cité

`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.

Preuve manuelle requise (attestation du responsable) · Texte cité

Ce rapport est une preuve automatisée et un élément d'auto-évaluation produits à partir des données vivantes de gestion des vulnérabilités du produit (SBOM, constats, état des SLA, décisions VEX, surveillance et activité d'audit) et des attestations du responsable. Il appuie une évaluation de la conformité ; ce n'est pas une certification. Les artefacts lisibles par machine (CycloneDX VDR, CSAF VEX, OpenVEX) sont disponibles depuis le menu Exporter du produit.

Généré par **VulnBeacon**