Modèle d'avis de sécurité CRA

Modèle d'avis de sécurité public pour les fabricants de produits comportant des éléments numériques, au titre du règlement (UE) 2024/2847 (règlement sur la cyberrésilience, CRA), annexe I partie II. À publier dès que la mise à jour de sécurité est disponible.

Horloge réglementaire distincte : les vulnérabilités activement exploitées doivent en outre être signalées via la plateforme de signalement unique de l'ENISA au titre de l'article 14 (alerte précoce sous 24 h / notification sous 72 h / rapport final sous 14 jours), applicable à partir du 11 septembre 2026.

Ce PDF est le guide de terrain ; le fichier de travail est le DOCX, et une variante Markdown lisible par machine est fournie pour les agents IA. Les trois fichiers sont gratuits sur orbiqhq.com/templates/cra-vulnerability-advisory-template — sans e-mail requis. Ce modèle est une aide, pas un conseil juridique.

Bloc d'en-tête de l'avis

Complétez chaque champ avant publication. Format de l'ID de l'avis : {{org_prefix}}-SA-{{year}}-{{sequence}}.

Champ	Valeur	Guidage
Titre de l'avis	{{advisory_title}}	Une ligne : <Produit> : <classe de faille> dans <composant> (<ID CVE>)
ID de l'avis	{{advisory_id}}	Stable, séquentiel, jamais réutilisé
ID CVE	{{cve_id}}	CVE-YYYY-NNNNN, ou « pending »
ID EUVD	{{euvd_id}}	EUVD-YYYY-NNNNN (base de données européenne des vulnérabilités de l'ENISA)
Sévérité	{{severity}} ({{cvss_base_score}})	none 0.0 / low 0.1-3.9 / medium 4.0-6.9 / high 7.0-8.9 / critical 9.0-10.0 (CVSS v4.0)
Vecteur CVSS v4.0	{{cvss_vector}}	La chaîne de vecteur complète, pas seulement le score
Statut d'exploitation	{{exploitation_status}}	none-known | poc-published | exploited-in-the-wild (ce dernier déclenche le signalement Art. 14 du CRA)
État de l'avis	{{advisory_state}}	draft | embargoed | published | updated | superseded | closed
Première publication (UTC)	{{published_date}}	Date ISO
Dernière mise à jour (UTC)	{{updated_date}}	Date ISO
Résumé	{{summary}}	2 à 4 phrases : la faille, l'impact pour l'attaquant et l'action la plus importante

Table des détails de la vulnérabilité

Impact et éléments factuels d'exploitation. L'annexe I partie II, point 4, exige une description de la vulnérabilité et des informations permettant aux utilisateurs d'identifier le produit concerné.

Champ	Contenu
Impact	{{impact_description}} — ce qu'un attaquant obtient en cas de succès, les préconditions (accès réseau, authentification, interaction utilisateur), les conditions limitantes dans les déploiements types
Détails d'exploitation	{{exploitation_details}} — base factuelle du champ de statut ; en cas d'exploitation active, mentionner le signalement au titre de l'article 14 via la plateforme de signalement unique
Remerciements	{{reporter_credit}} — nom/pseudonyme du découvreur, avec son consentement

Table des versions concernées et corrigées

Une ligne par gamme de produit. Couvrez TOUTES les gammes prises en charge ; indiquez explicitement les produits ou versions qui ne sont PAS concernés : {{not_affected_note}}.

Produit	Versions concernées	Version corrigée	Déploiement
{{product_name}}	{{affected_version_range}}	{{fixed_version}}	{{deployment_model}} (cloud | self-hosted | embedded/firmware)
{{product_name_2}}	{{affected_version_range_2}}	{{fixed_version_2}}	{{deployment_model_2}}

Mesures d'atténuation

Action recommandée : {{remediation_action}} — normalement « Passez à {{fixed_version}} ou une version ultérieure ». Précisez que la mise à jour de sécurité est gratuite (exigée pendant la période de support, annexe I partie II point 8) et si elle s'applique automatiquement. Solutions de contournement pour les clients qui ne peuvent pas appliquer le correctif immédiatement : {{mitigations}} — changements de configuration, restrictions réseau, désactivation de fonctionnalités. S'il n'en existe aucune, écrivez « Aucune solution de contournement n'est disponible ; la mise à niveau est la seule remédiation. » N'omettez jamais cette section.

Chronologie & journal des mises à jour

La chronologie de divulgation atteste d'un traitement des vulnérabilités « sans retard ». Ajoutez une ligne datée au journal pour chaque changement significatif (nouvelles versions concernées, exploitation observée, mesures d'atténuation révisées).

Date (UTC)	Événement / modification
{{date_reported}}	Vulnérabilité signalée par {{reporter_credit}}
{{date_triaged}}	Signalement trié et confirmé
{{date_cve_assigned}}	{{cve_id}} attribué
{{date_fix_released}}	Version corrigée {{fixed_version}} publiée
{{date_published}}	Avis publié (journal des mises à jour v1.0 : publication initiale)
{{update_date}}	Journal des mises à jour v{{update_version}} : {{update_description}}

Variante e-mail de notification

Subject: [{{severity_uppercase}}] Avis de sécurité {{advisory_id}} : {{advisory_title_short}}

Bonjour {{recipient_name}},

Nous avons publié un avis de sécurité concernant {{product_name}}.

Avis : {{advisory_id}} — {{advisory_title_short}}
CVE / EUVD : {{cve_id}} / {{euvd_id}}
Sévérité : {{severity}} (CVSS v4.0 {{cvss_base_score}})
Concerné : {{affected_version_range}}
Corrigé dans : {{fixed_version}}
Exploitation : {{exploitation_status}}

Ce que vous devez faire :
{{action_summary}}

L'avis complet, avec les mesures d'atténuation et la chronologie de divulgation :
{{advisory_url}}

Nous mettrons l'avis à jour en cas de changement significatif ; les abonnés à notre Trust Center reçoivent ces mises à jour automatiquement.

{{sender_name}}
Équipe sécurité, {{company_name}}
{{security_contact_email}}

Bloc de contact pour l'avis lui-même : signalez les vulnérabilités à {{security_contact_email}} (politique de divulgation coordonnée : {{cvd_policy_url}}). Clé PGP : {{pgp_key_url}} — empreinte {{pgp_fingerprint}}.

EXEMPLE REMPLI (fictif — à remplacer par vos propres données)

Bloc d'en-tête de l'avis — EXEMPLE (fictif)

Tous les noms, produits, versions, identifiants et événements sont fictifs, à titre d'illustration uniquement.

Champ	Valeur
Titre de l'avis	Aurivo Edge Gateway : exécution de code à distance non authentifiée dans l'API de synchronisation (CVE-2026-41337)
ID de l'avis	AURIVO-SA-2026-004
ID CVE	CVE-2026-41337
ID EUVD	EUVD-2026-08123
Sévérité	critical (9.3)
Vecteur CVSS v4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
Statut d'exploitation	none-known
État de l'avis	published
Première publication (UTC)	2026-06-24
Dernière mise à jour (UTC)	2026-07-01
Résumé	Une faille de désérialisation dans l'API de synchronisation des équipements d'Aurivo Edge Gateway permet à un attaquant réseau non authentifié d'exécuter du code arbitraire avec les privilèges du service. Aurivo Edge Gateway 3.8.2 corrige le problème. Effectuez la mise à niveau immédiatement ; une solution de contournement par configuration est disponible pour les déploiements qui ne peuvent pas appliquer le correctif cette semaine.

Table des détails de la vulnérabilité — EXEMPLE (fictif)

Champ	Contenu
Impact	Un attaquant disposant d'un accès réseau au port de l'API de synchronisation (8443/tcp par défaut) peut envoyer une charge utile forgée qui est désérialisée sans validation, aboutissant à une exécution de code à distance sous le compte de service aurivo-sync. Aucune authentification ni interaction utilisateur n'est requise. Les déploiements qui restreignent le port 8443 aux réseaux d'administration réduisent l'exposition, sans l'éliminer.
Détails d'exploitation	Nous n'avons pas connaissance d'une exploitation en conditions réelles, et aucune preuve de concept publique n'existe au moment de la publication. Si nous prenions connaissance d'une exploitation active, nous la signalerions via la plateforme de signalement unique du CRA conformément à l'article 14 et mettrions cet avis à jour.
Remerciements	Mira Lindqvist (chercheuse indépendante) — signalé via notre programme de divulgation coordonnée des vulnérabilités.

Table des versions concernées et corrigées — EXEMPLE (fictif)

Non concernés : Aurivo Cloud Console (l'API de synchronisation n'y est pas exposée) ; les versions d'Edge Gateway antérieures à 3.2.0 (le point de terminaison concerné a été introduit en 3.2.0).

Produit	Versions concernées	Version corrigée	Déploiement
Aurivo Edge Gateway	3.2.0 – 3.8.1	3.8.2	self-hosted
Aurivo Edge Gateway LTS	2.9.0 – 2.9.14	2.9.15	self-hosted

Mesures d'atténuation — EXEMPLE (fictif)

Action recommandée : passez à Aurivo Edge Gateway 3.8.2 (ou LTS 2.9.15) ou une version ultérieure. La mise à jour de sécurité est gratuite pour toutes les installations prises en charge et disponible via le canal de mise à jour standard. Solution de contournement : les déploiements qui ne peuvent pas appliquer le correctif immédiatement doivent restreindre l'accès au port TCP 8443 aux réseaux d'administration de confiance, ou désactiver l'API de synchronisation des équipements (sync.enabled = false dans gateway.conf ; redémarrage du service requis). La désactivation de la synchronisation suspend la distribution de la configuration du parc mais n'affecte pas le trafic du plan de données.

Chronologie & journal des mises à jour — EXEMPLE (fictif)

Date (UTC)	Événement / modification
2026-06-09	Vulnérabilité signalée par Mira Lindqvist (chercheuse indépendante)
2026-06-10	Signalement trié et confirmé
2026-06-12	CVE-2026-41337 attribué
2026-06-24	Versions corrigées 3.8.2 et 2.9.15 publiées
2026-06-24	Avis publié (journal des mises à jour v1.0 : publication initiale)
2026-07-01	Journal des mises à jour v1.1 : ajout de la plage concernée LTS 2.9.x et de la version corrigée 2.9.15

Variante e-mail de notification — EXEMPLE (fictif)

Subject: [CRITICAL] Avis de sécurité AURIVO-SA-2026-004 : RCE non authentifiée dans l'API de synchronisation d'Aurivo Edge Gateway

Bonjour Madame Berg,

Nous avons publié un avis de sécurité concernant Aurivo Edge Gateway.

Avis : AURIVO-SA-2026-004 — RCE non authentifiée dans l'API de synchronisation
CVE / EUVD : CVE-2026-41337 / EUVD-2026-08123
Sévérité : critical (CVSS v4.0 9.3)
Concerné : 3.2.0 – 3.8.1 et LTS 2.9.0 – 2.9.14
Corrigé dans : 3.8.2 / LTS 2.9.15
Exploitation : none-known

Ce que vous devez faire :
Mettez à niveau toutes les instances Edge Gateway auto-hébergées vers 3.8.2 (ou LTS 2.9.15) dès que possible. Si vous ne pouvez pas appliquer le correctif cette semaine, restreignez le port TCP 8443 aux réseaux d'administration de confiance ou désactivez l'API de synchronisation des équipements.

L'avis complet, avec les mesures d'atténuation et la chronologie de divulgation :
https://trust.aurivo.example/advisories/AURIVO-SA-2026-004

Nous mettrons l'avis à jour en cas de changement significatif ; les abonnés à notre Trust Center reçoivent ces mises à jour automatiquement.

Jonas Feld
Équipe sécurité, Aurivo Systems GmbH
security@aurivo.example