CRA-sjabloon voor kwetsbaarheidsadviezen

Het openbare beveiligingsadvies dat de Cyber Resilience Act vereist, klaar om in te vullen: kopblok met CVE- en EUVD-ID, CVSS v4.0-vector en misbruikstatus, tabellen voor getroffen en herstelde versies, mitigaties, tijdlijn en wijzigingslogboek — plus een volledig ingevuld voorbeeld.

Dit PDF is de veldgids. Het werkbestand is de DOCX; een machine-leesbare Markdown-variant is er voor AI-agents. Alle drie zijn gratis op orbiqhq.com/templates/cra-vulnerability-advisory-template — geen e-mail vereist.

Rechtsgrondslag: Verordening (EU) 2024/2847 (Cyber Resilience Act), bijlage I, deel II, punten 4 en 8; artikel 13 en artikel 14; Richtlijn (EU) 2022/2555 (NIS2), artikel 12, lid 2 (Europese kwetsbaarhedendatabank). Dit sjabloon is een hulpmiddel, geen juridisch advies.

Kopblok van het advies

Vul elk veld in vóór publicatie. Formaat van het advies-ID: {{org_prefix}}-SA-{{year}}-{{sequence}}.

Veld	Waarde	Toelichting
Titel van het advies	{{advisory_title}}	Één regel: <Product>: <type fout> in <component> (<CVE-ID>)
Advies-ID	{{advisory_id}}	Stabiel, oplopend, nooit hergebruikt
CVE-ID	{{cve_id}}	CVE-JJJJ-NNNNN, of 'pending'
EUVD-ID	{{euvd_id}}	EUVD-JJJJ-NNNNN (kwetsbaarhedendatabank van de EU, beheerd door ENISA)
Ernst	{{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)
CVSS v4.0-vector	{{cvss_vector}}	De volledige vectorstring, niet alleen de score
Misbruikstatus	{{exploitation_status}}	none-known | poc-published | exploited-in-the-wild (de laatste activeert de meldplicht van CRA-art. 14)
Status van het advies	{{advisory_state}}	draft | embargoed | published | updated | superseded | closed
Eerst gepubliceerd (UTC)	{{published_date}}	ISO-datum
Laatst bijgewerkt (UTC)	{{updated_date}}	ISO-datum
Samenvatting	{{summary}}	2-4 zinnen: de fout, de impact voor de aanvaller en de allerbelangrijkste actie

Tabel met kwetsbaarheidsdetails

Impact en onderbouwing van misbruik. Bijlage I, deel II, punt 4 vereist een beschrijving van de kwetsbaarheid en informatie waarmee gebruikers het getroffen product kunnen herkennen.

Veld	Inhoud
Impact	{{impact_description}} — wat een geslaagde aanvaller bereikt, de voorwaarden (netwerktoegang, authenticatie, gebruikersinteractie) en omstandigheden die misbruik in gangbare implementaties beperken
Details over misbruik	{{exploitation_details}} — de onderbouwing van het statusveld; bij misbruik in het wild: vermeld de melding onder artikel 14 via het centrale meldplatform
Vermelding	{{reporter_credit}} — naam/handle van de melder, met diens instemming

Tabel met getroffen en herstelde versies

Één rij per productlijn. Behandel ALLE ondersteunde lijnen; vermeld expliciet welke producten of versies NIET getroffen zijn: {{not_affected_note}}.

Product	Getroffen versies	Herstelde versie	Uitrolmodel
{{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}}

Mitigaties

Aanbevolen actie: {{remediation_action}} — normaal gesproken 'Werk bij naar {{fixed_version}} of later'. Vermeld dat de beveiligingsupdate kosteloos is (verplicht gedurende de ondersteuningsperiode, bijlage I, deel II, punt 8) en of hij automatisch wordt toegepast. Tijdelijke oplossingen voor klanten die niet direct kunnen patchen: {{mitigations}} — configuratiewijzigingen, netwerkbeperkingen, functies uitschakelen. Bestaan die niet, vermeld dan: 'Er zijn geen tijdelijke oplossingen; bijwerken is het enige herstel.' Laat deze sectie nooit weg.

Tijdlijn en wijzigingslogboek

De openbaarmakingstijdlijn toont aan dat u kwetsbaarheden 'onverwijld' afhandelt. Voeg bij elke materiële wijziging een gedateerde rij toe aan het wijzigingslogboek (nieuwe getroffen versies, waargenomen misbruik, herziene mitigaties).

Datum (UTC)	Gebeurtenis / wijziging
{{date_reported}}	Kwetsbaarheid gemeld door {{reporter_credit}}
{{date_triaged}}	Melding getrieerd en bevestigd
{{date_cve_assigned}}	{{cve_id}} toegekend
{{date_fix_released}}	Herstelde versie {{fixed_version}} uitgebracht
{{date_published}}	Advies gepubliceerd (wijzigingslogboek v1.0: eerste publicatie)
{{update_date}}	Wijzigingslogboek v{{update_version}}: {{update_description}}

E-mailvariant van de melding

```
Onderwerp: [{{severity_uppercase}}] Beveiligingsadvies {{advisory_id}}: {{advisory_title_short}}

Beste {{recipient_name}},

Wij hebben een beveiligingsadvies gepubliceerd dat {{product_name}} betreft.

Advies: {{advisory_id}} - {{advisory_title_short}}
CVE / EUVD: {{cve_id}} / {{euvd_id}}
Ernst: {{severity}} (CVSS v4.0 {{cvss_base_score}})
Getroffen: {{affected_version_range}}
Hersteld in: {{fixed_version}}
Misbruik: {{exploitation_status}}

Wat u moet doen:
{{action_summary}}

Het volledige advies, inclusief mitigaties en de openbaarmakingstijdlijn:
{{advisory_url}}

Wij werken het advies bij zodra er iets materieel verandert; abonnees van ons
Trust Center ontvangen die updates automatisch.

{{sender_name}}
Security Team, {{company_name}}
{{security_contact_email}}
```

Contactblok voor het advies zelf: meld kwetsbaarheden bij {{security_contact_email}} (CVD-beleid: {{cvd_policy_url}}). PGP-sleutel: {{pgp_key_url}} — vingerafdruk {{pgp_fingerprint}}.

INGEVULD VOORBEELD (fictief — vervang door uw eigen gegevens)

Kopblok van het advies — VOORBEELD (fictief)

Alle namen, producten, versies, identificatiecodes en gebeurtenissen zijn fictief en dienen uitsluitend ter illustratie.

Veld	Waarde
Titel van het advies	Aurivo Edge Gateway: niet-geauthenticeerde remote code execution in de sync-API (CVE-2026-41337)
Advies-ID	AURIVO-SA-2026-004
CVE-ID	CVE-2026-41337
EUVD-ID	EUVD-2026-08123
Ernst	critical (9.3)
CVSS v4.0-vector	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
Misbruikstatus	none-known
Status van het advies	published
Eerst gepubliceerd (UTC)	2026-06-24
Laatst bijgewerkt (UTC)	2026-07-01
Samenvatting	Een deserialisatiefout in de device-sync-API van Aurivo Edge Gateway stelt een niet-geauthenticeerde aanvaller met netwerktoegang in staat willekeurige code uit te voeren met de rechten van de service. Aurivo Edge Gateway 3.8.2 verhelpt het probleem. Werk direct bij; voor implementaties die deze week niet kunnen patchen is er een tijdelijke oplossing via de configuratie.

Tabel met kwetsbaarheidsdetails — VOORBEELD (fictief)

Veld	Inhoud
Impact	Een aanvaller met netwerktoegang tot de poort van de sync-API (standaard 8443/tcp) kan een geprepareerde payload sturen die zonder validatie wordt gedeserialiseerd, wat leidt tot remote code execution als het serviceaccount aurivo-sync. Authenticatie of gebruikersinteractie is niet nodig. Implementaties die poort 8443 beperken tot beheernetwerken verkleinen de blootstelling, maar heffen die niet op.
Details over misbruik	Wij zijn niet bekend met misbruik in het wild, en op het moment van publicatie bestaat er geen publieke proof-of-concept. Mochten wij kennis krijgen van actief misbruik, dan melden wij dat via het centrale CRA-meldplatform conform artikel 14 en werken wij dit advies bij.
Vermelding	Mira Lindqvist (onafhankelijk onderzoeker) — gemeld via ons programma voor gecoördineerde openbaarmaking van kwetsbaarheden.

Tabel met getroffen en herstelde versies — VOORBEELD (fictief)

Niet getroffen: Aurivo Cloud Console (de sync-API is daar niet benaderbaar); Edge Gateway-releases van vóór 3.2.0 (het getroffen endpoint is in 3.2.0 geïntroduceerd).

Product	Getroffen versies	Herstelde versie	Uitrolmodel
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

Mitigaties — VOORBEELD (fictief)

Aanbevolen actie: werk bij naar Aurivo Edge Gateway 3.8.2 (of LTS 2.9.15) of later. De beveiligingsupdate is kosteloos voor alle ondersteunde installaties en is beschikbaar via het reguliere updatekanaal. **Tijdelijke oplossing:** implementaties die niet direct kunnen patchen, doen er goed aan de toegang tot TCP-poort 8443 te beperken tot vertrouwde beheernetwerken, of de device-sync-API uit te schakelen (sync.enabled = false in gateway.conf; vereist een herstart van de service). Het uitschakelen van sync pauzeert de distributie van vlootconfiguratie, maar heeft geen gevolgen voor het dataplane-verkeer.

Tijdlijn en wijzigingslogboek — VOORBEELD (fictief)

Datum (UTC)	Gebeurtenis / wijziging
2026-06-09	Kwetsbaarheid gemeld door Mira Lindqvist (onafhankelijk onderzoeker)
2026-06-10	Melding getrieerd en bevestigd
2026-06-12	CVE-2026-41337 toegekend
2026-06-24	Herstelde versies 3.8.2 en 2.9.15 uitgebracht
2026-06-24	Advies gepubliceerd (wijzigingslogboek v1.0: eerste publicatie)
2026-07-01	Wijzigingslogboek v1.1: getroffen bereik LTS 2.9.x en herstelde versie 2.9.15 toegevoegd

E-mailvariant van de melding — VOORBEELD (fictief)

```
Onderwerp: [CRITICAL] Beveiligingsadvies AURIVO-SA-2026-004: niet-geauthenticeerde
RCE in de sync-API van Aurivo Edge Gateway

Beste mevrouw Berg,

Wij hebben een beveiligingsadvies gepubliceerd dat Aurivo Edge Gateway betreft.

Advies: AURIVO-SA-2026-004 - niet-geauthenticeerde RCE in de sync-API
CVE / EUVD: CVE-2026-41337 / EUVD-2026-08123
Ernst: critical (CVSS v4.0 9.3)
Getroffen: 3.2.0 - 3.8.1 en LTS 2.9.0 - 2.9.14
Hersteld in: 3.8.2 / LTS 2.9.15
Misbruik: none-known

Wat u moet doen:
Werk alle self-hosted Edge Gateway-instanties zo snel mogelijk bij naar 3.8.2
(of LTS 2.9.15). Kunt u deze week niet patchen, beperk dan TCP-poort 8443 tot
vertrouwde beheernetwerken of schakel de device-sync-API uit.

Het volledige advies, inclusief mitigaties en de openbaarmakingstijdlijn:
https://trust.aurivo.example/advisories/AURIVO-SA-2026-004

Wij werken het advies bij zodra er iets materieel verandert; abonnees van ons
Trust Center ontvangen die updates automatisch.
```

```
Jonas Feld
Security Team, Aurivo Systems GmbH
security@aurivo.example
```