CRA-Vorlage für Schwachstellen-Advisories

Vorlage für öffentliche Sicherheitshinweise (Security Advisories) für Hersteller von Produkten mit digitalen Elementen nach Verordnung (EU) 2024/2847 (Cyber Resilience Act, CRA), Anhang I Teil II. Zu veröffentlichen, sobald das Sicherheitsupdate verfügbar ist.

Davon getrennt läuft eine zweite regulatorische Uhr: Aktiv ausgenutzte Schwachstellen sind zusätzlich nach Artikel 14 über die zentrale Meldeplattform der ENISA zu melden (Frühwarnung binnen 24 h / Meldung binnen 72 h / Abschlussbericht binnen 14 Tagen); anwendbar ab dem 11. September 2026.

Dieses PDF ist der Feldleitfaden; die Arbeitsdatei ist das DOCX, und für KI-Agenten wird eine maschinenlesbare Markdown-Variante bereitgestellt. Alle drei Dateien sind kostenlos unter orbiqhq.com/templates/cra-vulnerability-advisory-template verfügbar — ohne E-Mail-Adresse. Diese Vorlage ist eine Hilfestellung, keine Rechtsberatung.

Kopfblock des Advisories

Füllen Sie vor der Veröffentlichung jedes Feld aus. Format der Advisory-ID: {{org_prefix}}-SA-{{year}}-{{sequence}}.

Feld	Wert	Hinweise
Titel des Advisories	{{advisory_title}}	Eine Zeile: <Produkt>: <Fehlerklasse> in <Komponente> (<CVE-ID>)
Advisory-ID	{{advisory_id}}	Stabil, fortlaufend, nie wiederverwendet
CVE-ID	{{cve_id}}	CVE-YYYY-NNNNN, oder „pending“
EUVD-ID	{{euvd_id}}	EUVD-YYYY-NNNNN (EU-Schwachstellendatenbank der ENISA)
Schweregrad	{{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-Vektor	{{cvss_vector}}	Vollständige Vektorzeichenfolge, nicht nur der Wert
Ausnutzungsstatus	{{exploitation_status}}	none-known | poc-published | exploited-in-the-wild (Letzteres löst die Meldepflicht nach CRA Art. 14 aus)
Advisory-Status	{{advisory_state}}	draft | embargoed | published | updated | superseded | closed
Erstveröffentlichung (UTC)	{{published_date}}	ISO-Datum
Zuletzt aktualisiert (UTC)	{{updated_date}}	ISO-Datum
Zusammenfassung	{{summary}}	2–4 Sätze: der Fehler, die Auswirkung für Angreifer und die wichtigste einzelne Maßnahme

Tabelle mit Schwachstellendetails

Auswirkung und Nachweise zur Ausnutzung. Anhang I Teil II Nummer 4 verlangt eine Beschreibung der Schwachstelle sowie Angaben, anhand derer Nutzer das betroffene Produkt identifizieren können.

Feld	Inhalt
Auswirkung	{{impact_description}} — was ein erfolgreicher Angreifer erreicht, welche Voraussetzungen bestehen (Netzwerkzugang, Authentifizierung, Nutzerinteraktion) und welche Bedingungen die Ausnutzbarkeit in typischen Installationen begrenzen
Details zur Ausnutzung	{{exploitation_details}} — Nachweisgrundlage für das Statusfeld; bei Ausnutzung in freier Wildbahn ist die Meldung nach Artikel 14 über die zentrale Meldeplattform zu vermerken
Danksagung	{{reporter_credit}} — Name/Handle der meldenden Person, mit deren Einwilligung

Tabelle betroffener und behobener Versionen

Eine Zeile je Produktlinie. Decken Sie ALLE unterstützten Linien ab; halten Sie ausdrücklich fest, welche Produkte oder Versionen NICHT betroffen sind: {{not_affected_note}}.

Produkt	Betroffene Versionen	Behobene Version	Bereitstellung
{{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}}

Abhilfemaßnahmen

Empfohlene Maßnahme: {{remediation_action}} — im Regelfall „Aktualisieren Sie auf {{fixed_version}} oder höher“. Halten Sie fest, dass das Sicherheitsupdate kostenlos ist (während des Unterstützungszeitraums vorgeschrieben, Anhang I Teil II Nummer 8) und ob es automatisch eingespielt wird. Workarounds für Kunden, die nicht sofort patchen können: {{mitigations}} — Konfigurationsänderungen, Netzwerkbeschränkungen, Deaktivieren von Funktionen. Falls es keine gibt, schreiben Sie: „Es sind keine Workarounds verfügbar; das Update ist die einzige Behebung.“ Lassen Sie diesen Abschnitt niemals weg.

Zeitleiste und Änderungsprotokoll

Die Offenlegungs-Zeitleiste belegt, dass Schwachstellen „unverzüglich“ behandelt wurden. Ergänzen Sie für jede wesentliche Änderung eine datierte Zeile im Änderungsprotokoll (neue betroffene Versionen, beobachtete Ausnutzung, überarbeitete Abhilfemaßnahmen).

Datum (UTC)	Ereignis / Änderung
{{date_reported}}	Schwachstelle gemeldet von {{reporter_credit}}
{{date_triaged}}	Meldung triagiert und bestätigt
{{date_cve_assigned}}	{{cve_id}} zugewiesen
{{date_fix_released}}	Behobene Version {{fixed_version}} veröffentlicht
{{date_published}}	Advisory veröffentlicht (Änderungsprotokoll v1.0: Erstveröffentlichung)
{{update_date}}	Änderungsprotokoll v{{update_version}}: {{update_description}}

Variante: Benachrichtigungs-E-Mail

Betreff: [{{severity_uppercase}}] Sicherheitshinweis {{advisory_id}}: {{advisory_title_short}}

Guten Tag {{recipient_name}},

wir haben einen Sicherheitshinweis zu {{product_name}} veröffentlicht.

```
Advisory: {{advisory_id}} — {{advisory_title_short}}
CVE / EUVD: {{cve_id}} / {{euvd_id}}
Schweregrad: {{severity}} (CVSS v4.0 {{cvss_base_score}})
Betroffen: {{affected_version_range}}
Behoben in: {{fixed_version}}
Ausnutzung: {{exploitation_status}}
```

Was Sie tun sollten:
{{action_summary}}

Vollständiges Advisory inklusive Abhilfemaßnahmen und Offenlegungs-Zeitleiste:
{{advisory_url}}

Wir aktualisieren das Advisory, sobald sich etwas Wesentliches ändert; Abonnenten unseres Trust Centers erhalten diese Aktualisierungen automatisch.

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

Kontaktblock für das Advisory selbst: Melden Sie Schwachstellen an {{security_contact_email}} (CVD-Richtlinie: {{cvd_policy_url}}). PGP-Schlüssel: {{pgp_key_url}} — Fingerprint {{pgp_fingerprint}}.

AUSGEFÜLLTES BEISPIEL (fiktiv — ersetzen Sie es durch Ihre eigenen Daten)

Kopfblock des Advisories — BEISPIEL (fiktiv)

Alle Namen, Produkte, Versionen, Kennungen und Ereignisse sind fiktiv und dienen ausschließlich der Veranschaulichung.

Feld	Wert
Titel des Advisories	Aurivo Edge Gateway: nicht authentifizierte Remote Code Execution in der Sync-API (CVE-2026-41337)
Advisory-ID	AURIVO-SA-2026-004
CVE-ID	CVE-2026-41337
EUVD-ID	EUVD-2026-08123
Schweregrad	critical (9.3)
CVSS-v4.0-Vektor	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
Ausnutzungsstatus	none-known
Advisory-Status	published
Erstveröffentlichung (UTC)	2026-06-24
Zuletzt aktualisiert (UTC)	2026-07-01
Zusammenfassung	Ein Deserialisierungsfehler in der Device-Sync-API des Aurivo Edge Gateway erlaubt einem nicht authentifizierten Angreifer im Netzwerk, beliebigen Code mit den Rechten des Dienstes auszuführen. Aurivo Edge Gateway 3.8.2 behebt das Problem. Aktualisieren Sie umgehend; für Installationen, die diese Woche nicht patchen können, steht ein Konfigurations-Workaround zur Verfügung.

Tabelle mit Schwachstellendetails — BEISPIEL (fiktiv)

Feld	Inhalt
Auswirkung	Ein Angreifer mit Netzwerkzugang zum Port der Sync-API (Standard 8443/tcp) kann eine präparierte Payload senden, die ohne Validierung deserialisiert wird — mit Remote Code Execution unter dem Dienstkonto aurivo-sync als Folge. Weder Authentifizierung noch Nutzerinteraktion sind erforderlich. Installationen, die Port 8443 auf Management-Netze beschränken, verringern die Exposition, beseitigen sie aber nicht.
Details zur Ausnutzung	Uns ist keine Ausnutzung in freier Wildbahn bekannt, und zum Zeitpunkt der Veröffentlichung existiert kein öffentlicher Proof of Concept. Sollten wir Kenntnis von aktiver Ausnutzung erlangen, melden wir dies gemäß Artikel 14 über die zentrale CRA-Meldeplattform und aktualisieren dieses Advisory.
Danksagung	Mira Lindqvist (unabhängige Forscherin) — gemeldet über unser Programm zur koordinierten Schwachstellenoffenlegung.

Tabelle betroffener und behobener Versionen — BEISPIEL (fiktiv)

Nicht betroffen: Aurivo Cloud Console (die Sync-API ist dort nicht exponiert); Edge-Gateway-Releases vor 3.2.0 (der betroffene Endpunkt wurde mit 3.2.0 eingeführt).

Produkt	Betroffene Versionen	Behobene Version	Bereitstellung
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

Abhilfemaßnahmen — BEISPIEL (fiktiv)

Empfohlene Maßnahme: Aktualisieren Sie auf Aurivo Edge Gateway 3.8.2 (bzw. LTS 2.9.15) oder höher. Das Sicherheitsupdate ist für alle unterstützten Installationen kostenlos und über den Standard-Updatekanal verfügbar. Workaround: Installationen, die nicht sofort patchen können, sollten den Zugriff auf TCP-Port 8443 auf vertrauenswürdige Management-Netze beschränken oder die Device-Sync-API deaktivieren (sync.enabled = false in gateway.conf; erfordert einen Neustart des Dienstes). Das Deaktivieren der Synchronisierung pausiert die Verteilung der Flottenkonfiguration, wirkt sich jedoch nicht auf den Datenverkehr der Data Plane aus.

Zeitleiste und Änderungsprotokoll — BEISPIEL (fiktiv)

Datum (UTC)	Ereignis / Änderung
2026-06-09	Schwachstelle gemeldet von Mira Lindqvist (unabhängige Forscherin)
2026-06-10	Meldung triagiert und bestätigt
2026-06-12	CVE-2026-41337 zugewiesen
2026-06-24	Behobene Versionen 3.8.2 und 2.9.15 veröffentlicht
2026-06-24	Advisory veröffentlicht (Änderungsprotokoll v1.0: Erstveröffentlichung)
2026-07-01	Änderungsprotokoll v1.1: LTS-2.9.x-Versionsbereich und behobene Version 2.9.15 ergänzt

Variante: Benachrichtigungs-E-Mail — BEISPIEL (fiktiv)

Betreff: [CRITICAL] Sicherheitshinweis AURIVO-SA-2026-004: nicht authentifizierte RCE in der Sync-API des Aurivo Edge Gateway

Guten Tag Frau Berg,

wir haben einen Sicherheitshinweis zu Aurivo Edge Gateway veröffentlicht.

```
Advisory: AURIVO-SA-2026-004 — nicht authentifizierte RCE in der Sync-API
CVE / EUVD: CVE-2026-41337 / EUVD-2026-08123
Schweregrad: critical (CVSS v4.0 9.3)
Betroffen: 3.2.0 – 3.8.1 und LTS 2.9.0 – 2.9.14
Behoben in: 3.8.2 / LTS 2.9.15
Ausnutzung: none-known
```

Was Sie tun sollten:
Aktualisieren Sie alle selbst gehosteten Edge-Gateway-Instanzen schnellstmöglich auf 3.8.2 (bzw. LTS 2.9.15). Wenn Sie diese Woche nicht patchen können, beschränken Sie TCP-Port 8443 auf vertrauenswürdige Management-Netze oder deaktivieren Sie die Device-Sync-API.

Vollständiges Advisory inklusive Abhilfemaßnahmen und Offenlegungs-Zeitleiste:
https://trust.aurivo.example/advisories/AURIVO-SA-2026-004

Wir aktualisieren das Advisory, sobald sich etwas Wesentliches ändert; Abonnenten unseres Trust Centers erhalten diese Aktualisierungen automatisch.

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