CRA Vulnerability Advisory Template

Version 1.0 · Updated 2026-07-03 · Free template · orbiqhq.com/templates/cra-vulnerability-advisory-template

Public security-advisory template for manufacturers of products with digital elements under Regulation (EU) 2024/2847 (Cyber Resilience Act), Annex I Part II. Publish once the security update is available. Separate regulatory clock: actively exploited vulnerabilities must additionally be reported via ENISA's single reporting platform under Article 14 (24h early warning / 72h notification / 14-day final report), applicable from 11 September 2026.

Advisory header block

Complete every field before publication. Advisory ID format: {{org_prefix}}-SA-{{year}}-{{sequence}}.

Field	Value	Guidance
Advisory title	*{{advisory_title}}*	One line: : in ()
Advisory ID	*{{advisory_id}}*	Stable, sequential, never reused
CVE ID	*{{cve_id}}*	CVE-YYYY-NNNNN, or 'pending'
EUVD ID	*{{euvd_id}}*	EUVD-YYYY-NNNNN (ENISA EU Vulnerability Database)
Severity	*{{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}}*	Full vector string, not just the score
Exploitation status	*{{exploitation_status}}*	none-known | poc-published | exploited-in-the-wild (the latter triggers CRA Art. 14 reporting)
Advisory state	*{{advisory_state}}*	draft | embargoed | published | updated | superseded | closed
First published (UTC)	*{{published_date}}*	ISO date
Last updated (UTC)	*{{updated_date}}*	ISO date
Summary	*{{summary}}*	2-4 sentences: the flaw, attacker impact, and the single most important action

Vulnerability details table

Impact and exploitation evidence. Annex I Part II point 4 requires a description of the vulnerability and information allowing users to identify the affected product.

Field	Content
Impact	*{{impact_description}}* — what a successful attacker achieves, preconditions (network access, authentication, user interaction), limiting conditions in typical deployments
Exploitation details	*{{exploitation_details}}* — evidence basis for the status field; if exploited in the wild, note the Article 14 report via the single reporting platform
Credit	*{{reporter_credit}}* — reporter name/handle, with consent

Affected and fixed versions table

One row per product line. Cover ALL supported lines; state explicitly which products or versions are NOT affected: {{not_affected_note}}.

Product	Affected versions	Fixed version	Deployment
{{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}}*

Mitigations

Recommended action: {{remediation_action}} — normally 'Upgrade to {{fixed_version}} or later'. State that the security update is free of charge (required during the support period, Annex I Part II point 8) and whether it applies automatically. Workarounds for customers who cannot patch immediately: {{mitigations}} — configuration changes, network restrictions, feature disablement. If none exist, state 'No workarounds are available; upgrading is the only remediation.' Never omit this section.

Timeline & update log

Disclosure timeline evidences vulnerability handling 'without delay'. Add a dated update-log row for every material change (new affected versions, exploitation observed, revised mitigations).

Date (UTC)	Event / Change
{{date_reported}}	Vulnerability reported by *{{reporter_credit}}*
{{date_triaged}}	Report triaged and confirmed
{{date_cve_assigned}}	*{{cve_id}}* assigned
{{date_fix_released}}	Fixed version *{{fixed_version}}* released
{{date_published}}	Advisory published (update log v1.0: initial publication)
{{update_date}}	Update log v*{{update_version}}*: *{{update_description}}*

Notification email variant

Subject: [{{severity_uppercase}}] Security advisory {{advisory_id}}: {{advisory_title_short}}

Hello {{recipient_name}},

We have published a security advisory affecting {{product_name}}.

Advisory: {{advisory_id}} — {{advisory_title_short}} CVE / EUVD: {{cve_id}} / {{euvd_id}} Severity: {{severity}} (CVSS v4.0 {{cvss_base_score}}) Affected: {{affected_version_range}} Fixed in: {{fixed_version}} Exploitation: {{exploitation_status}}

What you should do: {{action_summary}}

Full advisory, including mitigations and the disclosure timeline: {{advisory_url}}

We will update the advisory if anything material changes; subscribers to our Trust Center receive those updates automatically.

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

Contact block for the advisory itself: report vulnerabilities to {{security_contact_email}} (CVD policy: {{cvd_policy_url}}). PGP key: {{pgp_key_url}} — fingerprint {{pgp_fingerprint}}.

FILLED EXAMPLE (fictional — replace with your own data)

Advisory header block — SAMPLE (fictional)

All names, products, versions, identifiers, and events are fictional, for illustration only.

Field	Value
Advisory title	Aurivo Edge Gateway: unauthenticated remote code execution in the sync API (CVE-2026-41337)
Advisory ID	AURIVO-SA-2026-004
CVE ID	CVE-2026-41337
EUVD ID	EUVD-2026-08123
Severity	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
Exploitation status	none-known
Advisory state	published
First published (UTC)	2026-06-24
Last updated (UTC)	2026-07-01
Summary	A deserialization flaw in the device-sync API of Aurivo Edge Gateway allows an unauthenticated network attacker to execute arbitrary code with service privileges. Aurivo Edge Gateway 3.8.2 fixes the issue. Upgrade immediately; a configuration workaround is available for deployments that cannot patch this week.

Vulnerability details table — SAMPLE (fictional)

Field	Content
Impact	An attacker with network access to the sync API port (default 8443/tcp) can send a crafted payload that is deserialized without validation, resulting in remote code execution as the aurivo-sync service account. No authentication or user interaction is required. Deployments that restrict port 8443 to management networks reduce, but do not eliminate, exposure.
Exploitation details	We are not aware of exploitation in the wild, and no public proof-of-concept exists at the time of publication. Should we become aware of active exploitation, we will report it via the CRA single reporting platform in line with Article 14 and update this advisory.
Credit	Mira Lindqvist (independent researcher) — reported via our coordinated vulnerability disclosure programme.

Affected and fixed versions table — SAMPLE (fictional)

Not affected: Aurivo Cloud Console (the sync API is not exposed); Edge Gateway releases before 3.2.0 (the affected endpoint was introduced in 3.2.0).

Product	Affected versions	Fixed version	Deployment
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

Mitigations — SAMPLE (fictional)

Recommended action: Upgrade to Aurivo Edge Gateway 3.8.2 (or LTS 2.9.15) or later. The security update is free of charge for all supported installations and is available through the standard update channel. Workaround: deployments that cannot patch immediately should restrict access to TCP port 8443 to trusted management networks, or disable the

device-sync API (sync.enabled = false in gateway.conf; requires service restart). Disabling sync pauses fleet configuration distribution but does not affect data-plane traffic.

Timeline & update log — SAMPLE (fictional)

Date (UTC)	Event / Change
2026-06-09	Vulnerability reported by Mira Lindqvist (independent researcher)
2026-06-10	Report triaged and confirmed
2026-06-12	CVE-2026-41337 assigned
2026-06-24	Fixed versions 3.8.2 and 2.9.15 released
2026-06-24	Advisory published (update log v1.0: initial publication)
2026-07-01	Update log v1.1: added LTS 2.9.x affected range and fixed version 2.9.15

Notification email variant — SAMPLE (fictional)

Subject: [CRITICAL] Security advisory AURIVO-SA-2026-004: unauthenticated RCE in Aurivo Edge Gateway sync API

Hello Ms. Berg,

We have published a security advisory affecting Aurivo Edge Gateway.

Advisory: AURIVO-SA-2026-004 — unauthenticated RCE in the sync API CVE / EUVD: CVE-2026-41337 / EUVD-2026-08123 Severity: critical (CVSS v4.0 9.3) Affected: 3.2.0 – 3.8.1 and LTS 2.9.0 – 2.9.14 Fixed in: 3.8.2 / LTS 2.9.15 Exploitation: none-known

What you should do: Upgrade all self-hosted Edge Gateway instances to 3.8.2 (or LTS 2.9.15) as soon as possible. If you cannot patch this week, restrict TCP port 8443 to trusted management networks or disable the device-sync API.

Full advisory, including mitigations and the disclosure timeline: https://trust.aurivo.example/advisories/AURIVO-SA-2026-004

We will update the advisory if anything material changes; subscribers to our Trust Center receive those updates automatically.

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