

Vulnerability Deferral Dossier & Control-Investment Plan

AquaSCADA RTU-Link 4 (DEMO)



PREPARED FOR	AquaSCADA RTU-Link 4 (DEMO)	REFERENCE	19735f3f-c3fb-4411-a0ec-3770d1cb6ed7
GENERATED	2026-07-11T14:33:39.831933+00:00	SOURCE	workFlow:19735f3f-c3fb-4411-a0ec-3770d1cb6ed7

OVERVIEW

Executive Summary

Product: AquaSCADA RTU-Link 4 (DEMO) 4.9.2 — asset rtu-link-4-plant-gateway, exposure internet_via_management_plane, criticality high. CRA class (customer-asserted, not determined here): important_class_l.

5 DEFERRED FINDINGS	4 KEV-LISTED	4 ART. 14 FLAGGED	0 UNRESOLVED ANCHORS
------------------------	-----------------	----------------------	-------------------------

ANCHORING

Regulatory Basis

REGIME	ANCHOR	STATUS	ADJUDICATION BASIS
CRA	CRA:art_13	applicable	check_applicability(sector=manufacturing): CRA confidence 'likely', basis article 2 — notes verbatim: 'CRA is product-scoped (Art 2(1)): it applies to any manufacturer placing products with digital e...
CRA	CRA:art_14	applicable	check_applicability(sector=manufacturing): CRA confidence 'likely', basis article 2 — notes verbatim: 'CRA is product-scoped (Art 2(1)): it applies to any manufacturer placing products with digital e...
CRA	CRA:art_Annex I Part II (2)	applicable	check_applicability(sector=manufacturing): CRA confidence 'likely', basis article 2 — notes verbatim: 'CRA is product-scoped (Art 2(1)): it applies to any manufacturer placing products with digital e...
CRA	CRA:art_Annex I Part II (3)	applicable	check_applicability(sector=manufacturing): CRA confidence 'likely', basis article 2 — notes verbatim: 'CRA is product-scoped (Art 2(1)): it applies to any manufacturer placing products with digital e...
NIS2	NIS2:art_21	applicable	check_applicability: NIS2 confidence 'likely', basis article 2 — 'Manufacturing of critical products (medical devices, chemicals) covered as important entities'. Duty split noted: NIS2 binds the OPER...
NIS2	NIS2:art_23	applicable	Same NIS2 adjudication (likely, basis art_2). Entity-side incident reporting ladder (24h early warning / 72h notification / one-month final report) parallels the manufacturer-side CRA Art. 14 ladder...
GDPR	GDPR:art_32	applicable	check_applicability: GDPR confidence 'definite', basis article 2 ('applies to all sectors processing personal data'). The asset processes operator credentials (personal data), so the security-of-proc...

REGIME	ANCHOR	STATUS	ADJUDICATION BASIS
MACHINERY	MACHINERY:art_2	not_applicable	Not returned by check_applicability for this sector, and treated as non-applying with justification rather than silently dropped: the product is a remote-terminal/SCADA gateway (a component with digi...

CRA (EU) 2024/2847: Art. 14 reporting obligations apply from 2026-09-11; Annex I main obligations from 2027-12-11.

DEFERRALS

Deferral Records

CVE	COMPONENT	SCORE BASE → EFFECTIVE	KEV	ART. 14	DISPOSITION	DEFERRAL RATIONALE (CUSTOMER)	VALID UNTIL
CVE-2021-44228	pkg:maven/org.apache.logging.log4j/log4j-core@2...	10 → 10	yes	yes	under_investigation	Vendor HMI package embeds log4j 2.14; the vendor patch is certified only for firmware 5.x and the plant stays on 4.9 until the Q1-2027 shutdown.	2027-03-31
CVE-2014-0160	pkg:generic/openssl@1.0.1f	7.5 → 7.5	yes	yes	under_investigation	Management-plane TLS terminator appliance is end-of-sale; replacement budgeted next fiscal year.	2027-06-30
CVE-2023-44487	pkg:generic/apache-httpd@2.4.57	7.5 → 7.5	yes	yes	under_investigation	Reverse proxy reachable only from the engineering VLAN; upgrade rides the next maintenance window.	2026-12-31
CVE-2021-23337	pkg:npm/lodash@4.17.20	7.2 → 7.2	no	no	under_investigation	HMI web bundle rebuild pending vendor release cycle.	2026-12-31
CVE-2020-1472		5.5 → 5.5	yes	yes	under_investigation	AD domain controller is IT-managed outside the OT scope boundary; compensating: management-plane isolation.	

4 finding(s) are KEV-listed or actively exploited — once CRA Art. 14 applies (2026-09-11), actively exploited vulnerabilities carry a 24h reporting duty to ENISA/CSIRT. Deterministic fact-flag, not legal advice.

REMEDIATION

Remediation Plan (Control-Investment Simulation)

2

NET REDUCTION

2

FINDINGS IMPROVED

0

FINDINGS REGRESSED

3

IMMOVABLE

STEP	WHY PICKED	KIND	TARGET	MARGINAL	CUMULATIVE
1	positive_net	change_exposure	{"asset_id": "asset-inline"}	1	2

Findings improvable by at least one single control: 1 (the engine's de-duplicated union — never a sum across controls).

Best single investment: change_exposure {"asset_id": "asset-inline"} — improves 1 finding(s), total score reduction 1 (single-lever, measured against the fixed baseline).

Plan trimming & off-target regressions

Stopped: no_positive_marginal_gain; steps trimmed: 0.

CVE	REASON
CVE-2021-44228	no_rule_coverage
CVE-2021-23337	no_rule_coverage
CVE-2020-1472	no_rule_coverage

Per-investment improved and total_score_reduction are each measured independently against the same baseline; a finding improved by multiple investments is counted in each. Do NOT sum reductions across investments to estimate a combined remediation plan — controls overlap and combined/pairwise effects are not evaluated in this single-lever result. Use findings_improvable (a de-duplicated union) for the count of distinct findings at least one single control can lower.

Each plan step's marginal block is measured against the running state BEFORE that step (round-relative before/after), and step marginals do not sum to the plan total: off-target movement is captured only in the verified cumulative blocks. Read combined effect from cumulative and plan_summary.net_total_reduction, never by summing marginals.

Simulation is EXPERIMENTAL and unsigned. requires_review: ai_suggested_only; audit_ledger_entries: not_recorded.

PROVENANCE

VEX, Limits & Provenance

VEX EMITTED	no
VEX STATEMENTS	0
VEX REASON	The engine emitted one valid CycloneDX 1.6 fragment but it carries ZERO vulnerability statements: under vex_scope=adjusted_only no finding was contextually adjusted (zero rules fired), so every CVE was excluded as unadjusted and there is nothing to apply in Dependency-Track. The engine's inline VEX states findings as exploitable (re-prioritised, never suppressed); with no adjustments there are no statements to carry. A zero-statement VEX is not delivered as an artifact.
ENGINE VERSION	0.17.0
RULE LIBRARY	rules_v0.14.0
NO_REF	CVE-2020-1472
NO_ADJUSTMENT	CVE-2021-44228, CVE-2014-0160, CVE-2023-44487, CVE-2021-23337, CVE-2020-1472

Scope limits

The engine attested its EXPERIMENTAL display banner was present on the simulation output (display_banner_present), but the banner text was not carried into the submitted responses; the verbatim notice is in the engine output.

Scored on the inline context surface: verification-class attestations (asset_type, safety-PLC independence, segmentation-verified-by-test) are rejected requires_reviewed_context and did not contribute to any score. Registered ScoringContexts are operator-managed; zone- and safety-PLC-aware scoring is out of scope for this dossier.

Engine dispositions are decision support: under_investigation, review_required, non-authoritative. The only authoritative dispositions in this dossier are customer-held review decisions supplied at intake (review_decision_id), recorded verbatim.

Audit ledger entries: not_recorded.

DOCUMENT	SEGMENT	SHA-256	NOTE
CRA:art_13	https://eur-lex.europa.eu/eli/reg/2024/2847/oj#art_13	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833
CRA:art_14	https://eur-lex.europa.eu/eli/reg/2024/2847/oj#art_14	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833
CRA:art_Annex I Part II (2)	https://eur-lex.europa.eu/eli/reg/2024/2847/oj#art_Annex I Part II (2)	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833
CRA:art_Annex I Part II (3)	https://eur-lex.europa.eu/eli/reg/2024/2847/oj#art_Annex I Part II (3)	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833
NIS2:art_21	https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_21	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833
NIS2:art_23	https://eur-lex.europa.eu/eli/dir/2022/2555/oj#art_23	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833
GDPR:art_32	https://eur-lex.europa.eu/eli/reg/2016/679/oj#art_32	—	Publications Office of the European Union · EUR-Lex-Decision-2011-833

PROVENANCE

Citation Integrity

VALIDATION NOT APPLICABLE

CITATIONS 0
DRIFTED 0
ATTRIBUTION MISSING 0

no citation machinery ran for this report