EU Cyber Resilience Act Compliance Report

Automated assessment generated by Q-CRA Dashboard v1.0.0

Target:	demo.example-product.eu
Scan ID:	d6b6495c5578a60360e751365b60a7c4
Scanner:	Q-SCANNER v2.1.0
Scan Date:	2026-03-06T18:38:16.889529+00:00
Report Date:	2026-03-06 18:38 UTC

Overall Score:	84.2%
Articles Assessed:	12
Compliant:	6
Partially Compliant:	5
Non-Compliant:	1

Disclaimer: This report is generated automatically based on Q-SCANNER results and provides an indicative mapping to CRA articles. It does not constitute legal advice. For formal CRA conformity assessment, consult a qualified notified body.

1. Executive Summary

CRA Article	Category	Severity	Score	Status
Art.10(1)	Product Security	CRITICAL	90.0%	COMPLIANT
Art.10(2)	Vulnerability Management	CRITICAL	50.0%	NON_COMPLIANT
Art.10(3)	Update Management	HIGH	100.0%	COMPLIANT
Art.10(4)	Secure Defaults	HIGH	100.0%	COMPLIANT
Art.10(5)	Data Protection	CRITICAL	62.5%	PARTIAL
Art.10(6)	Attack Surface	HIGH	75.0%	PARTIAL
Art.11(1)	Reporting	CRITICAL	100.0%	COMPLIANT
Art.11(2)	User Communication	HIGH	100.0%	COMPLIANT
Art.13	Supply Chain	MEDIUM	83.3%	PARTIAL
Art.14	Supply Chain	MEDIUM	75.0%	PARTIAL
Annex I.1	Security Design	CRITICAL	100.0%	COMPLIANT
Annex I.2	Vulnerability Handling	HIGH	75.0%	PARTIAL

Key Findings

Critical gaps (1): Art.10(2) (Vulnerability Management)

Needs improvement (5): Art.10(5) (Data Protection), Art.10(6) (Attack Surface), Art.13 (Supply Chain), Art.14 (Supply Chain), Annex I.2 (Vulnerability Handling)

Post-Quantum Readiness: Your product does not implement post-quantum cryptography (NIST FIPS 203 ML-KEM / FIPS 204 ML-DSA). This exposes long-lived data to harvest-now-decrypt-later attacks. Q-CORE Systems recommends immediate PQC migration planning.

2. Detailed CRA Compliance Findings

Art.10(1) — Cybersecurity requirements for products with digital elements

Products shall be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks.

Score: 90.0% | **Status:** COMPLIANT | **Severity:** CRITICAL | **Category:** Product Security

Check	Status	Value	Detail
Tls Version	PASS	TLSv1.3	TLS 1.3 enforced, TLS 1.0/1.1 disabled
Cipher Strength	PASS	256-bit AES-GCM	AES-256-GCM with AEAD, no weak ciphers detected
Certificate Validity	PASS	Valid until 2026-03-15	X.509 certificate chain valid, OCSP stapling enabled
Protocol Security	PASS	HTTP/2 + HSTS	HSTS max-age=31536000, includeSubDomains
Key Exchange	WARNING	ECDHE-P256	Classical ECDHE only — no PQC hybrid key exchange (ML-KEM)

Art.10(2) — Vulnerability handling requirements

Manufacturers shall identify and document vulnerabilities, including third-party components.

Score: 50.0% | **Status:** NON COMPLIANT | **Severity:** CRITICAL | **Category:** Vulnerability Management

Check	Status	Value	Detail
Vulnerability Scan	WARNING	3 medium findings	CVE-2024-1234 (Medium), CVE-2024-5678 (Medium), CVE-2024-9012 (Low)
Cve Check	WARNING	2 unpatched CVEs	Known vulnerabilities in dependency libcrypto 3.0.x
Dependency Audit	PASS	148 deps audited	No critical vulnerabilities in direct dependencies
Sbom Present	FAIL	Not found	No SBOM (CycloneDX/SPDX) detected in product metadata

Art.10(3) — Security update delivery

Manufacturers shall ensure security updates are available for the expected product lifetime.

Score: 100.0% | **Status:** COMPLIANT | **Severity:** HIGH | **Category:** Update Management

Check	Status	Value	Detail
Update Mechanism	PASS	OTA + manual	Signed OTA update mechanism with rollback support
Patch Frequency	PASS	Monthly cycle	Regular monthly patch cycle with emergency hotfix capability
Auto Update Support	PASS	Enabled	Auto-update enabled by default, user can opt-out

Art.10(4) — Secure by default configuration

Products shall be delivered with secure default configurations, including the possibility to reset to original state.

Score: 100.0% | **Status:** COMPLIANT | **Severity:** HIGH | **Category:** Secure Defaults

Check	Status	Value	Detail
Default Credentials	PASS	No defaults	Unique credentials generated on first setup
Hardcoded Secrets	PASS	None detected	Static analysis found no hardcoded secrets or API keys
Secure Defaults	PASS	Enforced	Secure configuration shipped by default (firewall ON, debug OFF)
Factory Reset	PASS	Available	Factory reset clears all user data and returns to secure defaults

Art.10(5) — Data protection and minimization

Products shall protect the confidentiality and integrity of data, personal or otherwise.

Score: 62.5% | **Status:** PARTIAL | **Severity:** CRITICAL | **Category:** Data Protection

Check	Status	Value	Detail
Encryption At Rest	PASS	AES-256-XTS	Full-disk encryption with AES-256-XTS, key in TPM 2.0
Encryption In Transit	PASS	TLS 1.3 enforced	All data in transit protected by TLS 1.3
Data Minimization	WARNING	Partial	Telemetry collects device identifiers — review data minimization
Pqc Readiness	FAIL	Not implemented	No post-quantum cryptography (ML-KEM/ML-DSA) detected. Y2Q risk: harves

Art.10(6) — Attack surface minimization

Products shall minimize their attack surface, including external interfaces.

Score: 75.0% | **Status:** PARTIAL | **Severity:** HIGH | **Category:** Attack Surface

Check	Status	Value	Detail
Open Ports	WARNING	5 ports open	Ports 22, 80, 443, 8080, 8443 — review necessity of 8080
Unnecessary Services	WARNING	2 flagged	FTP and Telnet daemons detected — recommend removal
Api Exposure	PASS	Authenticated	All API endpoints require authentication (OAuth 2.0)
Network Segmentation	PASS	Implemented	Management and data planes properly segmented (VLAN)

Art.11(1) — Vulnerability reporting obligations

Manufacturers shall notify ENISA of actively exploited vulnerabilities within 24 hours.

Score: 100.0% | **Status:** COMPLIANT | **Severity:** CRITICAL | **Category:** Reporting

Check	Status	Value	Detail
Incident Response Plan	PASS	Documented	IRP version 3.2, last updated 2025-01-15, tested quarterly
Reporting Mechanism	PASS	Automated	Automated ENISA notification pipeline configured
Enisa Contact	PASS	Registered	ENISA CSIRT contact registered and verified

Art.11(2) — User notification of vulnerabilities

Manufacturers shall inform users about vulnerabilities and corrective measures without undue delay.

Score: 100.0% | **Status:** COMPLIANT | **Severity:** HIGH | **Category:** User Communication

Check	Status	Value	Detail
User Notification System	PASS	Multi-channel	Email + in-app + RSS advisory notifications
Advisory Publication	PASS	Public page	Security advisories published at /security/advisories
Disclosure Policy	PASS	90-day coordinated	Coordinated disclosure policy: 90-day window, bug bounty active

Art.13 — Obligations of importers

Importers shall ensure products comply with essential cybersecurity requirements.

Score: 83.3% | **Status:** PARTIAL | **Severity:** MEDIUM | **Category:** Supply Chain

Check	Status	Value	Detail
Ce Marking	PASS	Present	CE marking on product and documentation
Conformity Assessment	WARNING	In progress	Self-assessment completed, third-party audit scheduled Q2 2025
Documentation Complete	PASS	Complete	Technical documentation meets CRA Annex V requirements

Art.14 — Obligations of distributors

Distributors shall verify CE marking and conformity documentation before placing on the market.

Score: 75.0% | **Status:** PARTIAL | **Severity:** MEDIUM | **Category:** Supply Chain

Check	Status	Value	Detail
Supply Chain Verification	WARNING	Partial	First-tier suppliers verified, sub-tier verification pending
Distributor Checks	PASS	Documented	Distributor verification checklist in use

Annex I.1 — Essential cybersecurity requirements — Design

Products shall be designed with appropriate cybersecurity, protection from unauthorized access, and data confidentiality.

Score: 100.0% | **Status:** COMPLIANT | **Severity:** CRITICAL | **Category:** Security Design

Check	Status	Value	Detail
Auth Mechanism	PASS	MFA enforced	Multi-factor authentication required for all access
Access Control	PASS	RBAC	Role-based access control with principle of least privilege
Session Management	PASS	Secure	Secure session tokens, 30-min timeout, bind to IP
Input Validation	PASS	Server-side	Server-side input validation, parameterized queries, CSP headers

Annex I.2 — Essential cybersecurity requirements — Vulnerability handling

Coordinated vulnerability disclosure policy, SBOM, and effective security testing.

Score: 75.0% | **Status:** PARTIAL | **Severity:** HIGH | **Category:** Vulnerability Handling

Check	Status	Value	Detail
Sbom Present	FAIL	Not found	No SBOM (CycloneDX/SPDX) detected in product metadata
Coordinated Disclosure	PASS	Active	security@vendor, HackerOne bug bounty program
Security Testing	PASS	CI/CD integrated	SAST + DAST + SCA in CI/CD pipeline, weekly runs
Pentesting	PASS	Annual	Annual third-party penetration test, last: 2024-11-20

3. Recommendations

Priority 1 — Immediate Action Required

Art.10(2) — Sbom Present: No SBOM (CycloneDX/SPDX) detected in product metadata

Art.10(5) — Pqc Readiness: No post-quantum cryptography (ML-KEM/ML-DSA) detected. Y2Q risk: harvest-now-decrypt-later threat.

Annex I.2 — Sbom Present: No SBOM (CycloneDX/SPDX) detected in product metadata

Priority 2 — Improvement Recommended

Art.10(1) — Key Exchange: Classical ECDHE only — no PQC hybrid key exchange (ML-KEM)

Art.10(2) — Vulnerability Scan: CVE-2024-1234 (Medium), CVE-2024-5678 (Medium), CVE-2024-9012 (Low)

Art.10(2) — Cve Check: Known vulnerabilities in dependency libcrypto 3.0.x

Art.10(5) — Data Minimization: Telemetry collects device identifiers — review data minimization

Art.10(6) — Open Ports: Ports 22, 80, 443, 8080, 8443 — review necessity of 8080

Art.10(6) — Unnecessary Services: FTP and Telnet daemons detected — recommend removal

Art.13 — Conformity Assessment: Self-assessment completed, third-party audit scheduled Q2 2025

Art.14 — Supply Chain Verification: First-tier suppliers verified, sub-tier verification pending

Post-Quantum Cryptography Migration

The EU CRA emphasizes future-proof security. With NIST finalizing FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) standards, organizations should begin migration planning now. Q-CORE Systems provides full PQC migration tooling through Q-MIGRATOR and Q-HYBRID modules.

Appendix A: Methodology

This report was generated using Q-SCANNER automated security assessment mapped against the EU Cyber Resilience Act (Regulation (EU) 2024/2847). Each scanner check is mapped to one or more CRA articles based on the essential cybersecurity requirements defined in Article 10, Article 11, Article 13, Article 14, and Annex I of the regulation.

Scoring Methodology

Check Result	Score Weight	Article Status Threshold
PASS	1.0 (100%)	COMPLIANT: score >= 90%
WARNING	0.5 (50%)	PARTIAL: 60% <= score < 90%
FAIL	0.0 (0%)	NON-COMPLIANT: score < 60%

Appendix B: References

EU Regulation 2024/2847 — Cyber Resilience Act (CRA)

NIST FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

NIST FIPS 204 — Module-Lattice-Based Digital Signature Algorithm (ML-DSA)

ETSI EN 303 645 — Cyber Security for Consumer IoT

ISO/IEC 27001:2022 — Information Security Management

ENISA Guidelines on Vulnerability Disclosure

Report generated by Q-CRA Dashboard v1.0.0 | Q-CORE Systems | qcore.systems