

Unitronics Cyber Resilience Act Statement and Compliance Roadmap

Regulation (EU) 2024/2847 | Status September 2026 | Revision 01

1. Unitronics CRA commitment

Unitronics is actively implementing the requirements of Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA), across applicable products with digital elements placed on the European Union market.

The CRA establishes cybersecurity requirements covering the design, development, production, vulnerability handling, maintenance and support of products with digital elements throughout their lifecycle. The main CRA requirements will apply from 11 December 2027, while the mandatory vulnerability and severe-incident reporting requirements under Article 14 have applied since 11 September 2026.

Unitronics has established a structured CRA compliance program covering product security, vulnerability management, regulatory reporting, technical documentation and product lifecycle activities.

2. Current CRA readiness

As of September 2026, Unitronics has implemented the infrastructure and processes required to support the first applicable CRA milestone concerning vulnerability and incident reporting. Key measures currently in operation include:

- A formal Product Security Incident Response Team (PSIRT) and defined escalation responsibilities.
- A documented vulnerability reporting, assessment and coordinated disclosure process.
- A public cybersecurity portal allowing customers, researchers and other parties to report potential vulnerabilities.
- Defined processes for assessing reported vulnerabilities, including severity, applicability, exploitability and product impact.
- Procedures supporting the CRA reporting requirements for actively exploited vulnerabilities and severe security incidents.
- Security Advisory processes for communicating relevant product-security information to customers.
- Software Bill of Materials (SBOM) management for relevant products.
- Continuous monitoring and management of known vulnerabilities affecting applicable third-party software components.
- Internal traceability and evidence-retention processes supporting vulnerability investigation and regulatory compliance.

CRA Article 14 requires manufacturers to report certain actively exploited vulnerabilities and severe incidents, including an early warning within 24 hours and a notification within 72 hours of becoming aware. Reporting is performed through the CRA Single Reporting Platform established by ENISA.

3. CRA compliance roadmap

Period	CRA activity	Status
Completed / operational	Establish cybersecurity governance and PSIRT responsibilities	Implemented
Completed / operational	Establish public vulnerability-reporting mechanism	Implemented
Completed / operational	Vulnerability assessment and coordinated disclosure process	Implemented
Completed / operational	Security Advisory process	Implemented
Completed / operational	CRA Article 14 reporting process	Implemented
From 11 September 2026	Mandatory reporting of actively exploited vulnerabilities and severe security incidents	Operational
Completed / operational	Extend and mature SBOM and third-party component vulnerability management	Implemented
2026–2027	Product cybersecurity risk assessments against CRA Annex I	In progress
2026–2027	Review and implement applicable secure-by-design and secure-by-default requirements	In progress
2026–2027	Define and document product-specific security support periods	In progress
2026–2027	Review product security-update and vulnerability-remediation mechanisms	In progress
2026–2027	Prepare CRA technical documentation and compliance evidence	In progress
2026–2027	Determine applicable CRA product classifications and conformity-assessment routes	In progress
2027	Complete product-level CRA conformity assessments	Planned
By 11 December 2027	Complete implementation of applicable CRA requirements, including required product information, technical documentation, EU Declaration of Conformity and CE-marking obligations	Target: readiness by the applicable date
After 11 December 2027	Continuous vulnerability monitoring, security maintenance and lifecycle support	Ongoing

4. Vulnerability reporting and customer communication

Unitronics provides a dedicated cybersecurity portal for reporting suspected product-security vulnerabilities. Reports received through the vulnerability-reporting mechanism are evaluated through the Unitronics PSIRT process. Where appropriate, Unitronics communicates relevant vulnerability information, mitigations, corrective actions and affected product versions through Security Advisories.

Unitronics Cybersecurity Center

<https://www.unitronicsplc.com/cybersecurity/>

Vulnerability Handling and Coordinated Disclosure Policy

<https://www.unitronicsplc.com/cybersecurity/vulnerability-policy/>

Unitronics Security Advisories

<https://www.unitronicsplc.com/cybersecurity/security-advisories/>

5. SBOM and third-party components

Unitronics maintains Software Bills of Materials for relevant products as part of its product security and CRA compliance processes. SBOM information is used internally to support component identification, vulnerability monitoring, risk assessment and remediation activities.

The CRA does not generally require manufacturers to make product SBOMs publicly available or to provide them automatically to every customer. Where appropriate, a customer-facing SBOM may be provided upon justified request, considering the product scope, confidentiality and applicable internal approval requirements.

6. Product security and support

As part of the CRA implementation program, Unitronics progressively integrating CRA requirements into applicable product-development and lifecycle processes, including:

- Cybersecurity risk assessment.
- Secure product design and development.
- Protection against known exploitable vulnerabilities.
- Management of third-party components.
- Vulnerability monitoring and remediation.
- Security updates and corrective measures.
- Security-support period definition.
- Secure product documentation.
- Maintenance of product security throughout the applicable support period.

CRA Annex I requires products with digital elements to provide an appropriate level of cybersecurity based on risk and establishes vulnerability-handling requirements throughout the defined product support period.

7. Compliance position

Unitronics considers CRA compliance an ongoing product-lifecycle activity. At the present stage:

CRA Article 14 reporting requirements: Implemented and operational

Full product-level CRA requirements applicable from 11 December 2027: Implementation in progress

Unitronics' objective is to ensure that applicable products placed on the EU market meet the relevant CRA requirements by the applicable regulatory dates and that the necessary cybersecurity processes remain operational throughout the products' defined support periods.

8. Additional information

Customers requiring additional cybersecurity or CRA-related information for supplier qualification or regulatory assessment may contact Unitronics for the applicable documentation.

Available information may include, depending on product scope and confidentiality requirements:

- Cybersecurity policies and vulnerability-handling information.
- Security Advisories.
- Applicable customer-facing SBOM information.
- Cybersecurity certificates and supporting documentation.
- Product-specific security information.
- CRA compliance information as implementation progresses.

9. Official CRA references:

European Commission Cyber Resilience Act

<https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

Regulation EU 2024/2847

<https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

European Commission CRA reporting obligations

<https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>