BLACK DUCK®

CHECKLIST

EU CRA VULNERABILITY REPORTING CHECKLIST: SEPT. 2026 OBLIGATIONS

The European Union (EU) Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for software and hardware products sold in the EU. These requirements cover security by design, vulnerability handling, and ongoing maintenance obligations across the total product life cycle.

On September 11, 2026, the CRA entered the enforcement phase, requiring manufacturers, importers, and distributors of products with digital elements (PDEs) placed on the European market to notify ENISA and designated national CSIRTs of actively exploited vulnerabilities and severe security incidents associated with those PDEs.

Is your organization ready to meet CRA vulnerability reporting requirements? Our helpful checklist can help you prepare.

IN-SCOPE PRODUCTS

The CRA defines a product classification system that includes a default category for all software as well as stringent classifications based on primary product functions. It provides exclusions for products covered under alternative European cybersecurity or product safety regulations, such as the Medical Device Regulation or EU 2019/2144 for automotive safety. Penalties for nonconformance include fines that are a percentage of an organization's global revenue and potential removal of the PDE from the European market.

Products covered by the CRA include

- ☐ Products that contain software or firmware, or standalone software that is required for a connected product to function
- ☐ Products that are commercially distributed in the EU (free open source software without commercial activity is generally excluded)
- ☐ Products that are not already subject to specified industry-specific regulations
- ☐ Products already on the European market are in scope; the CRA requirements are not limited to new releases

MANDATORY REPORTING TIMELINES

The reporting timelines include

- ☐ **24 hours:** Manufacturers must file early warning of an actively exploited vulnerability or incident impacting SaaS or cloud components of a PDE within 24 hours of the manufacturer becoming aware of such an event, via the single reporting platform (SRP) provided by ENISA.
- ☐ **72 hours:** Manufacturers must provide a more detailed notification within 72 hours of becoming aware of an exploited vulnerability within their PDE that includes a description of the vulnerability, its impact, what corrective measures are being taken, and what mitigations a customer might take. This notification requirement includes vulnerabilities within integrated third-party components and incidents due to an active exploit impacting SaaS or cloud components supporting a PDE's operation.
- ☐ **14 days:** Manufacturers must provide a final report within 14 days after remediation becomes available covering the severity of the incident, the impact of the vulnerability, lessons learned, and process improvements. A full root cause analysis is also required for incidents impacting SaaS or cloud components of a PDE; this analysis deadline is one month after submitting the incident notification.

Reporting capabilities must be operational and tested before September 2026.

SBOM REQUIREMENTS

Software Bills of Materials (SBOMS) must

- ☐ Cover direct dependencies for every PDE placed on the European market, including product updates
- ☐ Be stored for potential review by market surveillance authorities

There is no requirement to share SBOMs with any third parties other than market surveillance authorities.

CONTINUOUS VULNERABILITY MONITORING

Manufacturers, distributors, and importers of PDEs should implement a continuous vulnerability monitoring process that can identify potential changes in software supply chain risk, as communicated via the European Vulnerability Database (EUVD) or other data sources as defined by the European Commission.

- ☐ Monitoring tools should prioritize potentially exploitable vulnerabilities but must also include integrated third-party components, including open source libraries.
- ☐ Manufacturers must monitor all products placed on the European market for the duration of the PDE's support period. For products containing integrated components from third parties, manufacturers must notify regulators and customers about exploitable vulnerabilities in those components.

REPORTING INFRASTRUCTURE

Manufacturers must file reports of actively exploited vulnerabilities via the SRP, and provide relevant details as defined by ENISA. Internal policies and playbooks must account for and describe vulnerability and incident reporting over the total product life cycle, including product support periods.

All cybersecurity decision-making must be documented, including tooling selection, vulnerability triage and disposition, scope of affected products, and external communications.

Required by September 11, 2026

- Vulnerability monitoring and processes
- SBOM-supported visibility
- Reporting workflows and timelines
- Disclosure and update processes

Due in 2027

- Cybersecurity requirements
- Secure by Design and Secure by Default process workflows with evidence
- Attack surface minimization
- Conformity assessments
- Data protection
- Resilience measures to protect device functionality

HOW BLACK DUCK CAN HELP

Black Duck provides application security tools designed to meet the stringent requirements of the CRA and its associated cybersecurity standards.

- Black Duck® SCA identifies third-party risk and continuously monitors the NVD, EUVD, and proprietary Black Duck Security Advisories (BDSAs) for emergent vulnerabilities and exploit information. This data allows for automated prioritization of risks for integrated components, allowing companies to meet their 24-hour reporting requirements.
- Coverity® Static Analysis identifies first-party risks that could become third-party risks if not properly addressed prior to shipping a product with digital elements to a customer within a supply chain.
- Defensics® Fuzzing identifies first- and third-party risk associated with cyberphysical devices, assemblies and subassemblies, and spare parts, allowing for real-world Secure by Default testing.

By helping teams identify open source and third-party components, track vulnerabilities, and establish repeatable processes for managing software risk, Black Duck supports the foundational practices needed to meet CRA vulnerability management and reporting obligations.

To learn how Black Duck can support your organization's CRA readiness efforts, contact us to start the conversation.

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.