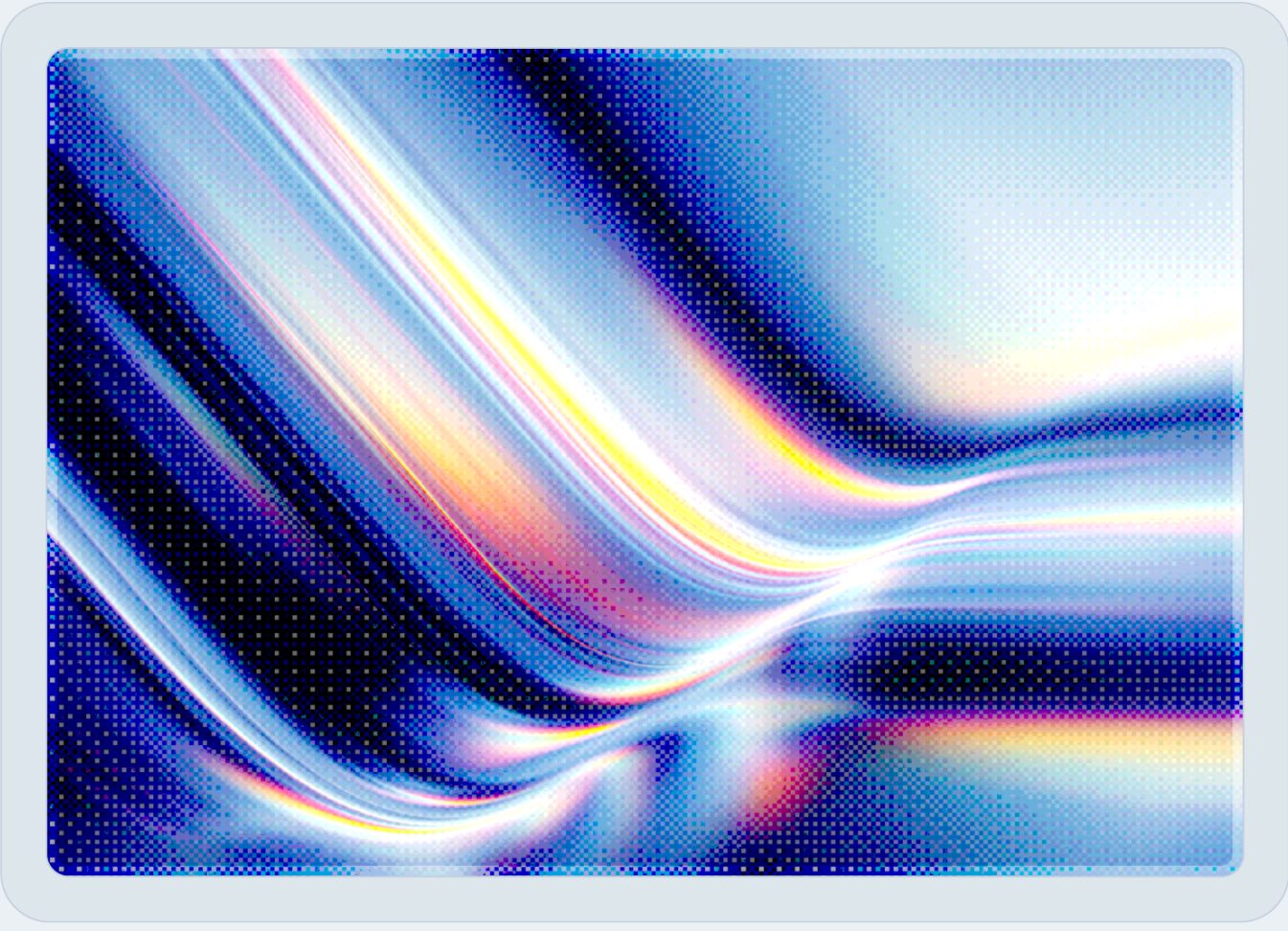
CSAI Foundation | Cloud Security Alliance

ENISA's CRA Reporting Platform Goes Live

Cyber Resilience Act Vulnerability and Incident Reporting Now Mandatory

2026-09-16

AI-assisted Rapid Research



CSAI

cloud security alliance®

Key Takeaways

The European Union Agency for Cybersecurity (ENISA) activated the Cyber Resilience Act (CRA) Single Reporting Platform (SRP) on September 11, 2026, the same date on which the CRA's vulnerability and incident reporting obligations became legally binding on manufacturers of products with digital elements sold in the EU market [1][2][3]. The platform lets manufacturers submit a single notification that ENISA and the relevant national Computer Security Incident Response Team (CSIRT) coordinator then distribute to other affected member states, replacing what would otherwise be a patchwork of separate national filings [2][3]. Manufacturers must now issue an early warning within 24 hours of becoming aware of an actively exploited vulnerability or a severe incident, follow with a detailed notification within 72 hours, and submit a final report within 14 days (for vulnerabilities) or one month (for incidents) once corrective or mitigating measures are available [2][3].

In practical terms, this launch converts the CRA from a forward-looking compliance obligation into an operational reality with immediate consequences for any organization that manufactures or maintains connected hardware or software sold into the EU. Because the initial release of the platform supports only manual web-form submission, without an API for automated filing, security and product teams need a documented, rehearsed internal process to gather the required technical detail and route it through the SRP inside the 24-hour window, rather than treating the deadline as aspirational. Organizations with mature vulnerability disclosure and incident response programs are likely best positioned to adapt. The compressed timelines and the CRA's broad product scope add further pressure: reporting obligations under Article 14, the duties at the center of the SRP, sit in the CRA's highest administrative fine tier, reaching up to €15 million or 2.5% of global annual turnover [4]. Combined with the compressed timelines and broad product scope, this means even well-run security programs will likely need to revisit ownership, escalation paths, and documentation practices specifically for CRA reportable events.

Background

The Cyber Resilience Act, which entered into force in December 2024 [1][3], establishes EU-wide cybersecurity requirements for products with digital elements, a category that spans consumer IoT devices, industrial control components, standalone software, and remote data-processing solutions that are logically or functionally connected to such products. The regulation follows a staged implementation schedule: reporting obligations under Article 14 became binding on September 11, 2026, while the

regulation's essential cybersecurity requirements, covering secure-by-design development, vulnerability handling processes, and conformity assessment, take full effect on December 11, 2027 [1][3]. This staged approach has the effect of giving ENISA and national authorities early visibility into the threat landscape while manufacturers continue building out compliant development practices, whether or not that sequencing was by original design.

The Single Reporting Platform addresses a coordination problem inherent to the CRA's multi-state reporting structure: a manufacturer selling into multiple member states could otherwise face separate reporting obligations to each state's national authority for the same vulnerability or incident. Under the SRP model, a manufacturer designates a CSIRT coordinator, generally located in the member state of its main establishment, defined as the location where cybersecurity decisions for the relevant products are predominantly made [3]. That coordinating CSIRT receives the initial submission and forwards it simultaneously to ENISA and to CSIRTs in other affected member states, except in exceptional circumstances [2]. ENISA Executive Director Juhan Lepassaar characterized the platform's purpose in terms of market-wide resilience, stating that streamlined reporting and information sharing on actively exploited vulnerabilities and severe incidents helps build a more resilient Digital Single Market [2].

Two categories of reportable events anchor the CRA's obligations. The first is an actively exploited vulnerability, meaning a flaw in a product with digital elements that is being exploited in the wild rather than merely disclosed or theoretical. The second is a severe incident, defined by its actual or potential significant impact on the security of the product or on user safety [3]. Manufacturers of connected hardware and software bear the primary reporting obligation starting September 11, 2026. Open-source software stewards, meaning organizations or projects that provide sustained support for open-source software incorporated into products with digital elements, face an identical set of obligations beginning December 11, 2027, giving the open-source ecosystem an additional grace period to build the organizational capacity that commercial manufacturers are nominally expected to have already built, even though, as the Security Analysis section below discusses, many commercial manufacturers have not yet operationalized that capacity for rapid external reporting [1][2].

The initial release of the SRP carries several practical limitations that manufacturers should factor into their compliance planning. Submissions currently occur only through a web interface, with no application programming interface available for automated or system-to-system filing, meaning organizations cannot yet integrate SRP reporting directly into existing security orchestration tooling [2]. The platform also launched in English only, with additional language support planned for later phases, and voluntary vulnerability reporting functionality, distinct from the mandatory reporting of actively exploited vulnerabilities, remains a future enhancement rather than a feature available at launch [2].

Security Analysis

The SRP's activation shifts the practical burden of CRA compliance from policy interpretation to operational execution, and the 24-hour early warning deadline is among the elements most likely to expose gaps in existing incident response workflows. Many incident response programs are designed around internal triage timelines that can run to several days, with external notification, to customers, regulators, or the public, typically following containment and impact assessment. The CRA inverts that sequence for actively exploited vulnerabilities and severe incidents: the clock starts when the organization becomes aware of the event, not when its investigation concludes, which means the early warning will frequently need to be filed before the manufacturer has a full picture of scope, root cause, or affected product lines. Security teams should expect their first SRP submission on any given event to be provisional by design, with the 72-hour follow-up notification serving as the venue for a more complete assessment as detailed in Article 14 [3].

The two reportable triggers, active exploitation and severe incidents, may also demand detection capabilities that not every manufacturer has systematically built into its vulnerability handling process, particularly around telemetry from deployed devices or correlation with external threat intelligence. Detecting that a vulnerability in a shipped product is being actively exploited in the wild typically requires direct telemetry from deployed devices, threat intelligence correlation with published indicators of compromise, or credible reporting from customers or security researchers. Organizations that have historically treated vulnerability disclosure as a one-way channel, receiving reports from external researchers and issuing patches on their own schedule, will need a complementary function that actively monitors for signs their own products are being targeted, since the CRA's clock starts at awareness regardless of how that awareness was obtained.

The financial exposure attached to non-compliance gives these operational gaps concrete weight. The CRA establishes a tiered administrative fine structure: non-compliance with the regulation's essential cybersecurity requirements under Annex I, together with the vulnerability-handling and reporting obligations under Articles 13 and 14, the duties at the center of the SRP, can draw fines of up to €15 million or 2.5% of an undertaking's total worldwide annual turnover, whichever is higher [4]. Non-compliance with other CRA obligations draws a lower tier of fines, up to €10 million or 2% of worldwide turnover [4]. Supplying incorrect, incomplete, or misleading information to notified bodies or market surveillance authorities carries a separate fine tier of up to €5 million or 1% of turnover [4]. Because these percentage-of-turnover figures apply to global revenue rather than EU-market revenue alone, the penalty structure can create meaningful exposure even for organizations for which the EU represents a minority of overall sales, and because SRP reporting obligations fall under the CRA's highest fine tier, the financial stakes of a missed or mishandled report are higher than a mid-tier compliance failure elsewhere in the regulation.

Recommendations

Immediate Actions

Manufacturers of products with digital elements sold into the EU market should confirm, without delay, that they have registered on the Single Reporting Platform and designated a CSIRT coordinator in their member state of main establishment, since this designation determines which national authority receives and routes their submissions [2][3]. Security and product teams should also conduct a rapid internal audit to identify which of their currently deployed products fall within CRA scope and verify that a named individual or team owns the responsibility for recognizing a reportable event and initiating the 24-hour early warning process, since ambiguity about ownership creates a real risk of missed deadlines under a 24-hour clock. Given that the SRP presently supports only manual web-form submission, teams should walk through a tabletop exercise of an actual SRP filing before a real event occurs, so that the mechanics of the platform are not being learned for the first time under deadline pressure.

Short-Term Mitigations

Organizations should extend their existing vulnerability management and incident response runbooks with a CRA-specific branch that triggers as soon as a candidate reportable event is identified, distinct from and running in parallel to internal containment and remediation workstreams. This branch should include pre-drafted templates for the 24-hour early warning that can be populated quickly with preliminary information, since the CRA does not require, and the compressed timeline does not allow for, a fully resolved investigation before that first notification is due. Because open-source software stewards face the same obligations beginning December 11, 2027, manufacturers that depend on third-party open-source components in their products with digital elements should begin engaging the maintainers of critical dependencies now, both to understand how those projects plan to meet their own future reporting obligations and to clarify how vulnerability information will flow between the open-source project and the manufacturer's own CRA reporting process.

Strategic Considerations

The SRP's launch marks the CRA's transition from a document-review compliance exercise into a live operational obligation, and organizations should treat this as a signal to revisit broader governance questions rather than a narrow reporting-mechanics problem. Product security, legal, and regulatory affairs functions should establish a standing coordination process for CRA events now, ahead of the more demanding December 11, 2027 deadline for the regulation's essential cybersecurity requirements,

since the operational muscle built for reporting, rapid internal awareness, cross-functional escalation, and accurate technical documentation under time pressure, will be directly reusable when the fuller compliance regime takes effect. Organizations operating across multiple regulatory regimes should also map CRA reporting obligations against parallel requirements under the Network and Information Security Directive 2 (NIS2) and, where applicable, the Digital Operational Resilience Act (DORA), since overlapping incident-reporting triggers across these regimes create both a risk of duplicated effort and an opportunity to consolidate detection and notification tooling around a single internal event-classification process.

CSA Resource Alignment

This development builds directly on findings in CSA's ENISA's SME Maturity Model Exposes a CRA Readiness Gap, which examined ENISA's own survey data showing that small and mid-sized manufacturers are broadly aware of the CRA but lack the resources and internal processes needed to comply with it. The SRP's activation converts that readiness gap from a future risk into a present compliance obligation: organizations identified in CSA's prior analysis as under-resourced for CRA compliance now face binding 24-hour reporting deadlines with real financial penalties attached, which sharpens the urgency of the process and staffing recommendations in that earlier research.

The SRP launch also connects to CSA's broader analysis of overlapping EU cybersecurity regimes, which has found that organizations subject to multiple regimes, including NIS2 and the CRA, benefit from treating compliance as a single integrated readiness program rather than addressing each regulation in isolation. That framing directly informs this note's recommendation to map CRA reporting triggers against NIS2 and DORA obligations rather than building a CRA-only notification process.

More broadly, the detection and disclosure practices the CRA now mandates fall within the Threat and Vulnerability Management domain of CSA's AI Controls Matrix (AICM) v1.1, whose control objectives around vulnerability identification, tracking, and timely remediation provide a structural foundation manufacturers can adapt to meet the CRA's specific reporting deadlines. Organizations that have already implemented AICM-aligned vulnerability management practices for AI-enabled products are well positioned to extend those same detection and escalation pathways to satisfy the SRP's 24-hour and 72-hour notification requirements.

References

[1] ENISA. "The CRA Single Reporting Platform Is Launched." European Union Agency for Cybersecurity, September 11, 2026.

[2] Help Net Security. "ENISA Launches CRA Single Reporting Platform." Help Net Security, September 14, 2026.

[3] Crowell & Moring. "It's Live: Cyber Resilience Act Reporting Is Mandatory as of Today, 11 September 2026." Crowell & Moring Client Alert, September 11, 2026.

[4] European Cyber Resilience Act. "Cyber Resilience Act Text, Article 64: Penalties." European Cyber Resilience Act, 2024.

[5] Cloud Security Alliance. "ENISA's SME Maturity Model Exposes a CRA Readiness Gap." Cloud Security Alliance, 2026.

[6] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.

