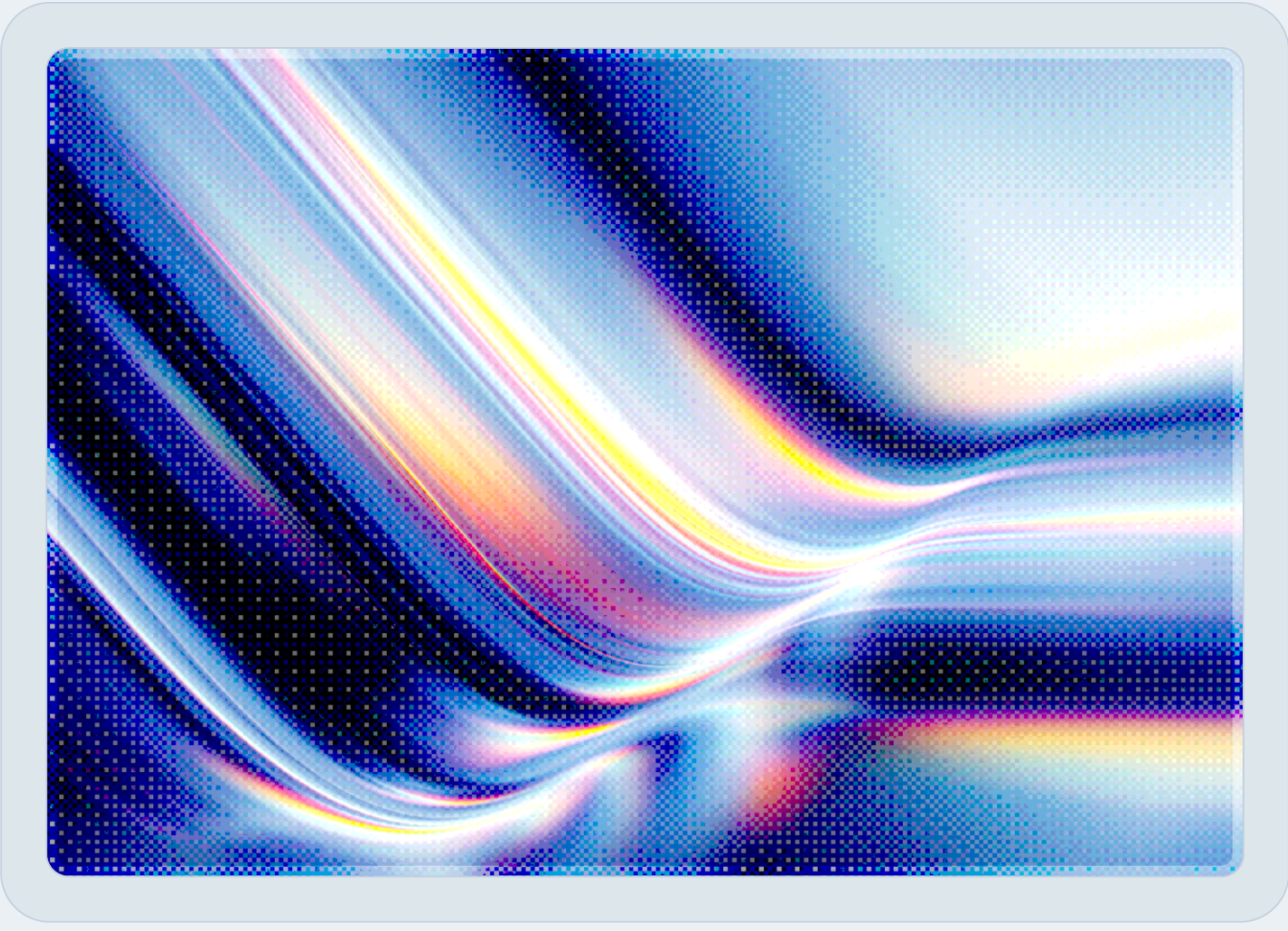
CSAI Foundation | Cloud Security Alliance

EU Cyber Resilience Act's Reporting Clock Starts

Security Implications and Guidance

2026-09-10

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- Starting September 11, 2026, manufacturers of products with digital elements sold into the EU must report actively exploited vulnerabilities and severe security incidents under Article 14 of the Cyber Resilience Act, on a three-stage clock: a 24-hour early warning, a 72-hour detailed notification, and a final report within 14 days (vulnerabilities) or one month (incidents) of a corrective measure becoming available [1][2].
- Reports flow through ENISA's Single Reporting Platform (SRP), a centralized system intended to route a single submission to both the manufacturer's national CSIRT and ENISA simultaneously, but as of September 8, 2026 the platform's public URL had not been published, voluntary reporting and API access were deferred with no date, and its countdown timer did not track the actual legal deadline [3][4].
- The regulation applies broadly to any manufacturer, EU-based or not, that places a networked hardware or software product on the EU market, and covers everything from consumer wearables to industrial control systems and the software components embedded inside them [2].
- Penalties for violating essential cybersecurity or reporting requirements reach €15 million or 2.5 percent of global annual turnover, whichever is higher, and regulators retain separate authority to restrict sales or compel product recalls independent of any fine [2].
- Because 98 percent of commercial applications contain open-source components, the practical bottleneck for most manufacturers is not legal interpretation but forensic reconstruction: knowing precisely what shipped in a given product version and when the organization first became aware of a vulnerability in it, a capability many software bills of materials (SBOMs) generated for audit purposes do not actually provide [5][8].
- A related ENISA survey of 194 organizations across 31 countries found that while two-thirds had heard of the CRA, incident response and product lifecycle management were the weakest of five assessed maturity domains, particularly at microenterprises, indicating that awareness of the deadline has outpaced operational readiness to meet it [6].

Background

The Cyber Resilience Act, formally Regulation (EU) 2024/2847, entered into force in December 2024 with a phased compliance timeline. Conformity assessment body notification requirements took effect in June 2026, and the regulation's full applicability, including essential cybersecurity requirements and CE marking obligations, arrives in December 2027. Article 14's reporting obligations sit ahead of that final deadline, and the practical effect of that sequencing is that the reporting pipeline, which depends on manufacturers already knowing what is in their products and how to escalate a problem quickly, is being tested in live conditions more than a year before the broader regime demands full technical documentation and certification [1][6].

That reporting pipeline becomes mandatory on September 11, 2026. From that date, any manufacturer of a product with digital elements sold into the EU market must notify the relevant authorities within 24 hours of becoming aware that a vulnerability in its product is being actively exploited, or that the product has suffered a severe incident affecting its ability to protect sensitive data or functions. A more detailed notification follows within 72 hours, and a final report is due within 14 days of a fix becoming available for a vulnerability, or within one month for an incident. Awareness, under ENISA's guidance, begins at "a reasonable degree of certainty" that exploitation is occurring, not at the point of absolute proof, and the clock runs through weekends and holidays regardless of platform availability or ongoing internal investigation [1][2].

The regulation's scope is deliberately broad. "Manufacturer" covers hardware producers, software developers, and providers of remote data processing solutions, whether they are headquartered inside the EU or simply sell a connected product into it, and the product side of that definition extends from consumer wearables and smart-home devices to industrial control systems and the open-source or commercial software libraries embedded inside them. Reports are meant to travel through ENISA's Single Reporting Platform, a system designed so that one submission satisfies notification duties to both the manufacturer's national Computer Security Incident Response Team and ENISA itself, avoiding the need to file separately with multiple authorities across member states [2][3].

Security Analysis

A regulatory deadline meeting an unfinished platform

In this note's assessment, the most immediate operational risk is not the reporting obligation itself but the state of the infrastructure meant to receive those reports. As of September 8, 2026, three days before the obligation took effect, the Single Reporting Platform's public access URL had still not been published, according to reporting tracking the rollout closely. Voluntary reporting functionality and API-based submission, both of which larger manufacturers had expected to use for integrating CRA reporting into existing incident response tooling, were deferred to a future release with no announced date. The platform's built-in countdown timer, intended to help filers track their remaining window, did not track the actual legal deadline and could show a notification as overdue before it legally was, and the system lacked a field to record when an organization first became aware of an issue, a gap that will not close until a later release [3][4]. None of this changes the legal obligation: the 24-hour and 72-hour clocks run from the moment of awareness, independent of whether the platform is reachable, fully featured, or displaying correct information. A manufacturer that cannot file because the platform is down or incomplete is not thereby excused from having attempted to meet the deadline, which puts a premium on documenting good-faith compliance efforts through whatever channel is available, including direct contact with the relevant national CSIRT [4].

The gaps above appear structural rather than incidental. ENISA has been building the SRP under public tender since procuring a development contractor, and functional and security testing were completed with participation from CSIRTs Network members shortly before launch, even as the public URL, voluntary reporting, API access, and the awareness-timestamp field remained unresolved [3][4][7]. That combination, tested infrastructure paired with unresolved access and interoperability gaps, is what manufacturers are contending with three days out. Manufacturers that assumed the platform would function as a mature, general-availability system likely need to recalibrate expectations mid-deadline. Organizations that have not already identified their coordinating CSIRT, created EU Login accounts for primary filers and backups, or drafted a notification template covering the mandatory 24-hour fields are starting that preparatory work with the deadline already in effect rather than in advance of it [4].

The harder problem: knowing what shipped, and when you knew

Beneath the platform issues sits a structural problem that a functioning SRP will not solve on its own. Article 14 compliance depends on an organization being able to answer, on demand and under a legal deadline, exactly which product version a customer received, which components that version contained, and the precise moment the organization first had reasonable certainty that one of those components

carried an exploited vulnerability. That question is difficult to answer for most software, even where documentation exists. Because open-source components appear in roughly 98 percent of commercial applications, this is not an edge case affecting a handful of specialized vendors; it is close to a universal condition of modern software supply chains, and it means nearly every manufacturer selling into the EU inherits vulnerability disclosure timing from upstream projects it does not control [5][8].

SBOMs generated primarily to satisfy an audit or a one-time compliance checkbox commonly describe a snapshot that goes stale the moment a dependency is updated, which means the document an organization can produce may already misrepresent what is actually running in production by the time a reporting clock starts. This gap matters more under the CRA than it did under prior compliance regimes because the timelines are unusually tight relative to how vulnerability remediation actually happens today: industry data on application vulnerability remediation puts the average time to fix a high- or critical-severity flaw at roughly 55 days, a pace that sits comfortably outside the CRA's 72-hour notification window and underscores that notification, not remediation, is what the early clock actually demands [5][9]. Two structural approaches address this gap. Organizations can instrument their own build pipelines to regenerate SBOMs automatically rather than on a periodic audit cycle, assign named ownership for vulnerability triage decisions, and treat component provenance as an ongoing supply chain property rather than a document produced once for a customer or regulator. Alternatively, organizations can shift toward consuming pre-vetted, already-attested open-source components where the provenance and disclosure-handling questions are answered upstream before the component is integrated, reducing the amount of forensic reconstruction the manufacturer itself must perform when a vulnerability surfaces [5]. Manufacturers that have not tested their own readiness are advised to run a concrete exercise: pick a product version shipped six months ago and measure, in wall-clock time, how long it takes to identify every component in it and cross-reference that list against newly disclosed vulnerabilities. Organizations for which that exercise takes days rather than hours have already identified their compliance gap before the first real incident forces the question [5].

A readiness gap concentrated among smaller manufacturers

Survey data ENISA published alongside its SME Cyber Resilience Maturity Assessment Model reinforces that the readiness gap is not evenly distributed. Across 194 organizations surveyed in 31 countries, two-thirds reported having heard of the CRA, but maturity scoring across five domains, governance and documentation, risk management and secure-by-design practices, vulnerability and patch management, product lifecycle management, and workforce awareness, showed medium-sized firms scoring roughly a full point higher than microenterprises on a five-point scale in every domain. Incident response and product lifecycle management were consistently the weakest domains, and the gap was most pronounced at the smallest organizations [6]. That pattern is consistent with microenterprises being less likely to have a dedicated security function capable of standing up a 24-hour reporting process on short

notice, though the survey itself measured maturity-domain scores rather than staffing levels directly. More than 70 percent of surveyed organizations specifically requested practical templates rather than additional framework documentation, and 142 of the 194 respondents cited a need for financial support to close the gap, suggesting that the barrier for smaller manufacturers is less a knowledge deficit than a resourcing and execution one [6]. This finding extends, in this note's reading, beyond the SME population directly surveyed: larger manufacturers and enterprise buyers routinely depend on smaller suppliers for components and subsystems, so under-resourced upstream vendors may become the practical constraint on a larger organization's own CRA reporting timeline even when that larger organization has invested heavily in its own readiness.

Recommendations

Immediate Actions

Organizations that have not already done so should complete the platform-independent preparatory work the reporting clock now demands, since none of it requires the SRP itself to be functional. Create EU Login accounts for the individuals designated as primary filers and their backups, and confirm multi-factor authentication is configured so account access is not itself a point of failure during an active incident. Identify the specific national CSIRT that will coordinate notifications based on where the organization has its main establishment, and open a direct line of contact with that CSIRT as a fallback channel given the platform's unresolved gaps. Draft a notification template in advance covering the fields the 24-hour early warning requires, including a working title, a factual summary, affected product identification, and the circumstances under which the issue was detected, so that the first real filing is a matter of populating a template rather than composing a report under deadline pressure.

Short-Term Mitigations

Beyond the immediate filing mechanics, security and product teams should close the forensic gap between what compliance documentation claims and what the organization can actually demonstrate under deadline. Test SBOM currency directly by selecting a product version shipped several months ago and timing how long it takes to produce an accurate, complete component inventory for it; treat any result measured in days rather than hours as an active compliance risk rather than a documentation nicety. Establish a named, on-call rotation with explicit weekend and holiday coverage for CRA awareness and reporting decisions, since the 24-hour and 72-hour clocks do not pause for either, and confirm that whoever holds that rotation has clear authority to trigger a report without waiting on a broader approval chain. Review supply chain contracts with component and subsystem suppliers to

confirm they are contractually obligated to notify the organization promptly of vulnerabilities in what they provide, since the organization's own reporting clock starts on becoming aware, and a slow supplier can quietly consume most of a 24-hour window before the organization even learns there is something to report.

Strategic Considerations

Over the longer term, organizations should treat CRA reporting readiness as one instance of a broader shift in how vulnerability disclosure timelines are regulated, rather than a standalone EU compliance project. Integrate CRA reporting workflows into existing incident response plans alongside parallel obligations under NIS2, national breach notification laws, and comparable regimes such as U.S. federal Known Exploited Vulnerabilities catalog deadlines, so that a single incident does not trigger duplicated, inconsistent internal processes across different regulatory tracks. Invest in automated, continuously regenerated SBOM tooling rather than periodic audit-driven documentation, since the provenance question the CRA asks of manufacturers is structurally the same question increasingly asked by defense contractors, healthcare regulators, and enterprise procurement teams, making the investment reusable well beyond this specific deadline. Finally, extend supplier maturity assessment into standing third-party risk programs rather than treating it as a one-time CRA onboarding exercise, given that ENISA's own survey data shows the weakest link in the regulated ecosystem is consistently the smaller supplier whose product lifecycle and incident response processes have not yet caught up to what the regulation now requires of the manufacturers who depend on them.

CSA Resource Alignment

ENISA's SME Maturity Model Exposes a CRA Readiness Gap [6] examines the same ENISA survey data referenced in this note's Security Analysis section in greater depth, breaking down the five maturity domains against specific CRA obligations and offering a phased roadmap oriented toward resource-constrained manufacturers. It should be read alongside this note by any organization assessing supplier readiness within a third-party risk program, particularly since the forensic and process gap this note describes, knowing what shipped and when an organization became aware of a problem in it, recurs across the two maturity domains ENISA's survey scored weakest: incident response and product lifecycle management.

The AI Controls Matrix (AICM) v1.1 [10] provides the governing control framework for the vulnerability and patch management, and governance and documentation, gaps this note identifies. AICM's Threat and Vulnerability Management domain calls for continuous, current asset and component inventory as a

prerequisite for vulnerability handling, which is precisely the SBOM-currency capability that separates organizations able to meet the CRA's 24-hour and 72-hour clocks from those that cannot, and its Audit and Assurance domain provides the documentation discipline needed to demonstrate, after the fact, exactly when an organization became aware of an issue. Organizations building a CRA readiness program should treat an AICM-aligned control assessment, rather than a CRA-specific checklist built from scratch, as the more durable foundation, since the underlying control objectives extend to reporting regimes beyond the CRA.

References

[1] Freshfields. "Cyber Resilience Act reporting obligations take effect on 11 September 2026." Freshfields, September 2026.

[2] Crowell & Moring. "EU Cyber Resilience Act: September 11, 2026 Reporting Deadline." Crowell & Moring, 2026.

[3] European Commission. "Cyber Resilience Act – Reporting obligations." Shaping Europe's Digital Future, European Commission, 2026.

[4] cyberresilienceact.eu. "Eighteen Days to CRA Reporting: What You Can Prepare Before the Platform Opens on 11 September 2026." cyberresilienceact.eu, September 8, 2026.

[5] BleepingComputer. "The EU CRA's Real Question: What Shipped, and When Did You Know?." BleepingComputer, September 2026.

[6] Cloud Security Alliance. "ENISA's SME Maturity Model Exposes a CRA Readiness Gap." Cloud Security Alliance, July 15, 2026.

[7] cyberresilienceact.eu. "CRA Reporting: 24h, 72h & 14-Day Deadlines (Article 14)." cyberresilienceact.eu, 2026.

[8] Black Duck. "2026 Open Source Security and Risk Analysis Report." Black Duck, 2026.

[9] Edgescan. "2026 Vulnerability Statistics Report." Edgescan, 2026.

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

