

Eurosmart's position paper on Article 14 of the Cyber Resilience Act

October 2026

Executive summary

The successful entry into force of Article 14 of the Cyber Resilience Act¹ on September 11th, 2026, is jeopardized by the lack of clarity in the meaning of “actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI) which are to be reported by manufacturers.

These ambiguities will substantially hamper the successful implementation of Article 14 starting from September 11th. These will lead to fragmentation across Member States regarding security monitoring of the EU market, will create market distortion within the EU market as manufacturers will be subject to diverging national interpretations and ultimately will expose them to legal risks resulting from uncertainty.

Eurosmart notes that further clarification on these aspects has so far received limited attention, be in the FAQ² or the CRA guidance³. Therefore, Eurosmart calls on the European Commission to provide clarification on the ambiguities outlined below as soon as possible.

Issue#1: “severe incident having an impact on the security of a product with digital elements” (SI)

Recital (68) reads “[...] Severe incidents having an impact on the security of the product with digital elements, on the other hand, refer to situations where a cybersecurity incident affects the development, production or maintenance processes of the manufacturer in such a way that it could

¹ REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

² <https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act-implementation-frequently-asked-questions>

³ COMMUNICATION TO THE COMMISSION Approval of the content of the draft Communication from the Commission - Commission guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act) - <https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation>

result in an increased cybersecurity risk for users or other persons. Such a severe incident could include a situation where an attacker has successfully introduced malicious code into the release channel via which the manufacturer releases security updates to users.”. The wording “cybersecurity” in this recital is ambiguous as it may be understood in two ways, giving different meaning of what is “severe incident having an impact on the security of a product with digital elements” (SI):

- **Either as the consequence of the risk**, e.g. a risk with cybersecurity consequences. In such cases, any risk, regardless of its nature will be covered. This could include the theft of design documentation in premises, cases where the reference documentation or harmonized standard used for conformity assessment appears not to appropriately cover essential cybersecurity requirements, changes to the harmonized standard used for conformity assessment, the emergence of new non-technical risk factors;
- **Or as the nature of the risk**, meaning that e.g. theft of design documentation in premises, cases where the reference documentation or harmonized standard used for conformity assessment appears not to appropriately cover essential cybersecurity requirements, changes to harmonized standard used for conformity assessment, or the emergence of new non-technical risk factors would not qualify as a “severe incident having an impact on the security of a product with digital elements” (SI).

This ambiguity should be cleared to avoid wrong interpretations by manufacturers, legal risks for them, and ultimately a gap in the monitoring of security events by CSIRT. This is particularly relevant to ensure a robust and consistent cybersecurity level across the EU, and in line with the full hazard approach as defined in NIS2.

Hence, Eurosmart recommends the clarification in recital (68) that cybersecurity risks should be understood as risks whose consequences are of cybersecurity nature.

Recital (68) is instrumental to scope the meaning of “severe incident having an impact on the security of a product with digital elements” (SI) for manufacturer. Likewise, interpretation should be provided to manufacturers regarding how other events should be considered:

- Should a privacy issue be considered as a “severe incident having an impact on the security of a product with digital elements” (SI), and if yes under which conditions?
- Should an issue related to the safety of the product be considered as a “severe incident having an impact on the security of a product with digital elements” (SI), and if yes under which conditions?
- Should a cyberattack operated by an AI agent on its own (AI Agent escaping its planned use and carrying out malicious operation see ^{4, 5, 6 and 7}) be considered as a “severe incident having an impact on the security of a product with digital elements” (SI), and if yes under which conditions?

⁴ <https://abcnews.com/Business/ai-models-fake-identities-trick-humans-cyberattack-officials/story?id=135384187>

⁵ <https://www.forbes.com/sites/thomasbrewster/2026/09/22/huge-cyberattack-uses-anthropic-and-deepseek-ai-to-target-100-companies/>

⁶ <https://global.techradar.com/fr-fr/pro/security/rubygems-accuse-des-agents-dopenai-davoir-lance-une-attaque-massive-contre-son-infrastructure>

⁷ <https://www.theguardian.com/technology/2026/sep/11/openai-agents-rubygems-malicious-packages>

Hence, Eurosmart recommends clarifying these questions.

Recital (68) restricts “severe incident having an impact on the security of a product with digital elements” (SI) to incident which “[...] affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons”. However, this clarification is not recalled in the legal definition of “severe incident having an impact on the security of a product with digital elements” (SI) in Articles 3 and 14. This absence may lead once more to wrong interpretations by manufacturers, legal risks for them, and ultimately a gap in the monitoring of security events by CSIRT.

Therefore, Eurosmart recommends reiterating that “severe incident having an impact on the security of a product with digital elements” (SI) only applies to incident which “[...] affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons.”

Issue#2: vulnerabilities in the environment of the product with digital elements

The product with digital elements may be designed to operate and be used in a particular environment comprising hardware and software. The product’s security, as per the cybersecurity risk assessment, may rely on some security properties of its environment. As such, a vulnerability or incident in the product’s environment may impact the security of the product with digital elements itself.

These events, when they occur, do not fall in any of the two events “severe incident having an impact on the security of a product with digital elements” (SI) or “actively exploited vulnerability” (AEV) as they:

- Do not “[...] affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons” (recital 68) as required for “severe incident having an impact on the security of a product with digital elements” (SI);
- Are not contained in the product as required for “actively exploited vulnerability” (AEV) – Article 14.1.

In addition, the environment in which the product with digital elements is used is under the sole control of the user and is not under the control of the product nor the manufacturer. Thus, it is the user’s responsibility to ensure security patches and security recommendations pertaining to its environment (e.g. operating systems) are correctly applied and followed.

Hence, Eurosmart recommends to be explicit that any vulnerability or incident in the product’s environment does not create any obligations for the manufacturer of the product with digital element.

Issue#3: “actively exploited vulnerability” (AEV)

Further guidance should be provided to manufacturers to help them determine whether they are facing an “actively exploited vulnerability” (AEV) and therefore should report it.

In some cases, the manufacturer may not have the necessary information (1) to ascertain whether a “vulnerability” is “actively exploited”, or (2) required to carry out the reporting obligation (early warning, notification, final report). Therefore, the manufacturer could end up in a situation where its product is facing an “actively exploited vulnerability” (AEV) and thus has the obligation to report it, but (1) is not able to determine that such a “vulnerability” is effectively “actively exploited”, or (2) has determined that the product is facing an “actively exploited vulnerability” (AEV) but is unable to provide the technical information required to carry out the reporting obligation (early warning, notification, final report). In such a case, the manufacturer has to meet an obligation for which it is liable but that it cannot fulfill.

This is the case, for instance, of professional products intended to be used by professional customers (i.e. not a consumer), for professional activities. These professional products are intended to be installed and run on the customer environment (IT infrastructure, IT network and premise). However, given the sensibility of its activities, customers confidentiality and IT cybersecurity rules may prohibit them from sharing information with the manufacturer about a vulnerability in the product. In turn, this prevents the manufacturer from (1) determining whether a “vulnerability” is “actively exploited” or (2) providing the technical information required to carry out the reporting obligation (early warning, notification, final report). Examples of such situations include complex software providing payment services sold to financial institutions or merchants’ websites, or complex software for the management of national digital identity or tax systems sold to States.

Therefore to support the manufacturers facing such a situation, a **guidance shall be prepared clarifying:**

- **That where the manufacturer cannot get the necessary information from its users or customers to determine whether a “vulnerability” is “actively exploited”, the manufacturer has no obligations under Article 14, as the manufacturer cannot be “aware” of an “actively exploited vulnerability”. Alternatively, the guidance should clarify how a manufacturer could determine whether a “vulnerability” is “actively exploited” in case it cannot have relevant information from its customers or users. To do so, this guidance should describe how to determine the likelihood that a “vulnerability” is “actively exploited” based on a list of objective and verifiable criteria that are accessible to and verifiable by the manufacturers.**
- **Where the manufacturer cannot get the necessary information from its users or customers to carry out the reporting obligation (early warning, notification, final report), the manufacturer has no obligation to provide these information under Article 14, and it is not liable for the absence of these information.**

Issue#4: interplay between “actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI)

Eurosmart recommends clarifying the following aspects:

- What is the core difference between “actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI)?
- Considering the CRA, it seems that:
 - “actively exploited vulnerability” (AEV) is something intrinsic to the product with digital elements;
 - “severe incident having an impact on the security of a product with digital elements” (SI)? to be an exogenous factor to the product with digital elements;

If correct, this interpretation should be explicitly confirmed.

- Additionally, can an event simultaneously qualify both as “actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI)? So, are “actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI) always different in essence? This clarification is important for the manufacturers to know whether they shall notify the event in the Single Reporting Platform (SRP) once, or twice (“actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI)).

Issue#5: content of final report of “actively exploited vulnerability” (AEV) and “severe incident having an impact on the security of a product with digital elements” (SI)

As per Article 14.2(c), in case of “actively exploited vulnerability” (AEV) the manufacturer shall submit “[...] a final report, no later than 14 days after a corrective or mitigating measure is available, [...]”. In addition, this final report shall contain “[...] details about the security update or other corrective measures that have been made available to remedy the vulnerability.” (Article 14.2(c)(iii)). However, as per Article 71, the provisions of the CRA related to vulnerability handling shall only apply to products with digital elements placed on the market from December 11th, 2027. This means that for reporting of “actively exploited vulnerability” (AEV) on a product with digital elements placed on the market before December 11th, 2027, the reporting process is not applicable as a whole, as vulnerability handling is not required,

This raises the following questions for the reporting of “actively exploited vulnerability” (AEV) on a product with digital elements placed on the market before December 11th, 2027:

- The final report is required “[...] no later than 14 days after a corrective or mitigating measure is available [...]”. As vulnerability handling is not required, does it mean that the reporting of “actively exploited vulnerability” (AEV) on a product with digital elements placed on the market before December 11th, 2027, can omit the final report where no corrective or mitigating measure is envisioned?
- The final report shall contain “[...] details about the security update or other corrective measures that have been made available to remedy the vulnerability.”. As vulnerability handling is not required, if the final report is submitted, does it mean that the reporting of “actively exploited vulnerability” (AEV) on product with digital elements placed on the market before December 11th, 2027, can omit the “[...] details about the security update or other corrective measures that have been made available to remedy the vulnerability”?

Similar issues have also been identified for “severe incident having an impact on the security of a product with digital elements” (SI). As per Article 14.4(c)(iii), in case of “severe incident having an impact on the security of a product with digital elements” (SI) the manufacturer shall submit a final report containing “[...] applied and ongoing mitigation measures”. However, as per Article 71, the provisions of the CRA related to vulnerability handling shall only apply to products with digital elements placed on the market from December 11th, 2027. Hence, it means that for reporting of “severe incident having an impact on the security of a product with digital elements” (SI) on a product with digital elements placed on the market before December 11th, 2027, the reporting process is not applicable as a whole, as vulnerability handling is not required.

This raises the following question for the reporting of “severe incident having an impact on the security of a product with digital elements” (SI) on product with digital elements placed on the market before December 11th, 2027:

- The final report shall contain “[...] applied and ongoing mitigation measures”. As vulnerability handling is not required, when the final report is submitted, does it mean that the reporting of “severe incident having an impact on the security of a product with digital elements” (SI) on a product with digital elements placed on the market before December 11th, 2027, can omit the “[...] applied and ongoing mitigation measures”?

Eurosmart recommends clarifying that for products placed on the market before December 11th, 2027, the provisions of:

- **Article 14.2(c)(iii) requiring providing in the final report “[...] details about the security update or other corrective measures that have been made available to remedy the vulnerability.” (for “actively exploited vulnerability” – AEV);**
- **Article 14.4(c)(iii) requiring providing in the final report “[...] applied and ongoing mitigation measures” (for “severe incident having an impact on the security of a product with digital elements” - SI);**

are not applicable.

Issue#6: “actively exploited vulnerability” (AEV) shall be understood in the light of the context of use and risk profile

As per Article 3.42, an “actively exploited vulnerability” (AEV) is defined as “[...] a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner”.

However, this definition does not consider the product intended purpose declared by the manufacturer, which also covers the operational environment where it should be used. That operational environment also includes the level of «dangers/risks» in the operational environment against which the product provides protections (e.g. product provides protection of data integrity in an uncontrolled environment versus product provides data integrity protection in a controlled physical environment). These parameters are relevant and should be considered when determining if a “vulnerability” shall qualify as “actively exploited”.

The approach underpinning the harmonized standards for the CRA under preparation for the various product categories considers a “risk profile” or “security level” as input to define the applicable security requirements for the conformity assessment of products. In turn, this “risk profile” or “security level” matches the intended purpose of the product and therefore it is commensurate with the level of risks and dangers the product will face during its lifetime. Concretely, this “risk profile” or “security level” reflects the level of dangers or risks in the operational environment against which the product shall provide protections. This level of dangers or risks implied by the product intended purpose is directly linked to the necessary will of a malicious actor to exploit a vulnerability, which is named its “attack potential”. This “attack potential” reflects the needed investment for a malicious actor to successfully exploit a vulnerability, as it can be translated into the required devices, materials, skills, time and ultimately money. The “attack potential” to which the product shall resist is defined so that it is not viable for a malicious actor to successfully exploit a vulnerability, i.e. it costs far more than the expected benefits in the light of the product intended purpose.

Hence, the qualification of a “vulnerability” as an “actively exploited vulnerability” (AEV) should duly consider the “attack potential” implied by the product intended purpose. It may not be appropriate to report a “vulnerability” as “actively exploited” if its exploitation requires an “attack potential” higher than the one defined for the product’s intended purpose. In such a case the malicious actor would face a negative yield, as the exploitation of the vulnerability would be more expensive than the expected benefits, which in turn will deter that malicious actor to exploit that vulnerability.

Therefore, Eurosmart recommends clarifying that “actively exploited vulnerabilit[ies]” (AEV) are only those which can be successfully exploited by a malicious actor having the same “attack potential” as the one implied by the product intended purpose. A “vulnerability” whose exploitation requires an “attack potential” higher than the one implied by the product’s intended purpose shall not qualify as “actively exploited vulnerability” (AEV) .

Issue#7: Reporting obligations are currently not limited in time

Currently the reporting obligations are not limited in time. However, it may not be realistic to require manufacturers to fulfill their reporting obligations for products indefinitely. As such, an obligation that is unlimited in time could lead to ever-growing costs, which may divert investment from the development of new products towards the maintenance of support functions.

Hence, a limit in time should be defined for the reporting obligations to provide clarity to manufacturers. A good approach would be to limit this obligation until the support period of the last product that has been placed on the market has expired.

Therefore, Eurosmart recommends clarifying that the reporting obligation applies until the support period of the last product that has been placed on the market has expired.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.



www.eurosmart.com



@Eurosmart_EU



@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 471 34 59 64 | mail Contact@eurosmart.com