enisa | CRA SINGLE REPORTING PLATFORM

CRA Single Reporting Platform Factsheet

How to Report Incidents and Actively Exploited Vulnerabilities via the **Single Reporting Platform** (SRP)

What?

As of 11 September 2026, the Cyber Resilience Act (CRA) requires manufacturers to report actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements sold in the EU market.

The CRA also requires open-source software stewards to report those events to the extent that they are involved in the development of products with digital elements.

For whom?

Manufacturers

Open-source software (OSS) stewards

What are your new reporting obligations?

The CRA Single Reporting Platform (SRP) is an online tool for manufacturers and open-source software stewards to meet the obligation to report actively exploited vulnerabilities and severe incidents. Designed to simplify EU reporting obligations, the CRA SRP is an electronic system to report only once to communicate to all relevant authorities. The platform incorporates security measures to protect confidentiality.

Each notification allows sending information automatically to your national CSIRT that initially receives the notification, the other national CSIRTs where the Product with digital elements is available, and to the EU Agency for Cybersecurity (ENISA).

Which national CSIRT should you report to?

In general, the national CSIRT to which you should report through the SRP is primarily determined by your main location of establishment. Article 14(7) of the CRA provides detailed information allowing you to identify the national CSIRT to report to.

What events are you obliged to report?

- **Actively Exploited Vulnerabilities:** Vulnerabilities in products with digital elements that are known to be currently exploited by a malicious actor, in accordance with Article 3(42) of the CRA.
- **Severe Incidents:** Incidents that have a severe impact on the security of the product with digital elements (e.g., compromising availability, authenticity, integrity, or confidentiality) in accordance with Article 3(44); the criteria for severity are defined in Article 14(5).

When do you need to report such events?

The reporting process starts the moment you, as a manufacturer or OSS steward, become aware of an active exploitation of a vulnerability or severe incident. Adhering to the following timelines:

Early Warning

- Within **24 hours** of becoming aware of the vulnerability or incident.

Actively Exploited Vulnerability / Severe Incident Notification

- Within **72 hours** of becoming aware, providing general information and an initial assessment.

Final Report

- For **vulnerabilities**: No later than **14 days** after a corrective measure (e.g. patch) is available.
- For **severe incidents**: Within 1 month after the submission of the 72-hour Actively Exploited Vulnerability / Severe Incident Notification

CRA SINGLE REPORTING PLATFORM

What happens once notifications are submitted?

Once notifications are submitted, the CSIRT initially receiving the notification will then disseminate the information without delay to other relevant CSIRTs in EU Member States where the product is also available. The notification is simultaneously made available to ENISA.

National CSIRTs will also share some information with their respective market surveillance authorities to enable them to fulfil their enforcement obligations.

Can dissemination of information be delayed?

Yes, under exceptional circumstances the dissemination of information may be delayed, pursuant to Article 16(2) of the CRA. Commission Delegated Regulation (EU) 2026/881 further specifies the conditions under which the dissemination of notifications may be delayed.

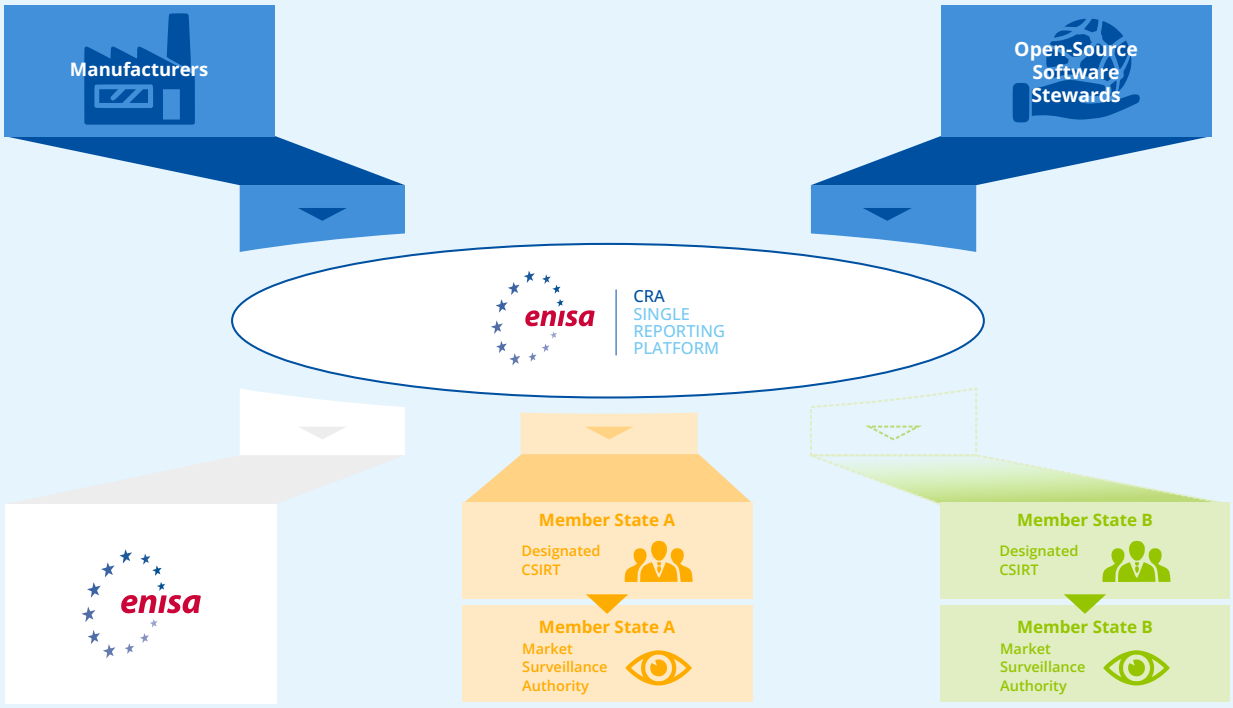
How would you use the platform?

1 Login

2 Select National CSIRT

3 Complete info and submit

Simple submission flow



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

For further information consult the ENISA SRP FAQ page https://www.enisa.europa.eu/cra-srp, which also includes references to the 'European Commission's guidance on the CRA', which in section 9.1 includes further clarifications on reporting obligations.

For support, please contact: cra-srp-helpdesk@enisa.europa.eu