The Countdown Is On: Are You Ready for the First CRA Requirements?

As of 11 September 2026, the first mandatory CRA requirements will apply: manufacturers must report actively exploited vulnerabilities and severe security incidents within the required timeframes via the central EU reporting platform – for many companies, this will be the first real test of their CRA readiness.

Why act now?

The reporting obligations under Article 14 of the CRA require companies to quickly identify and assess security events, establish clear responsibilities, and provide reliable technical information within the required timeframes. Unclear responsibilities, communication channels, and documentation can cost valuable time when an incident occurs and increase regulatory, operational, and reputational risks.

Who Is Affected?

The reporting obligation applies to all manufacturers of digital products placed on the EU market.

This particularly applies to:

- Software manufacturers
- IoT and smart device manufacturers
- Machinery manufacturers with connected control systems
- Manufacturers of medical devices incorporating software (unless superseded by sector-specific legislation)
- Industry 4.0 component manufacturers
- Manufacturers of network components and embedded systems

Important: Manufacturers outside the EU are also affected if they offer their products on the EU market.

What Must Be Reported?

ACTIVELY EXPLOITED VULNERABILITIES

A report is required when:

- a vulnerability in one of the manufacturer's own products becomes known,
- the vulnerability is being actively exploited by threat actors, and
- the manufacturer becomes aware of the exploitation.

Important: Not every vulnerability is reportable. A CVE entry or the findings of a penetration test alone do not trigger a reporting obligation.

SEVERE SECURITY INCIDENTS

Security incidents affecting product security may also be reportable if they have a significant impact, for example:

- Supply chain attacks
- Compromised firmware updates
- Attacks targeting update servers
- Distribution of malware through products

www.tuv.com/cra

TÜV Rheinland

What Are the Reporting Deadlines?

THE CRA ESTABLISHES A MULTI-STAGE REPORTING PROCESS.

WITHIN 24 HOURS

Early Warning:
Initial information about the security incident must be submitted.

WITHIN 72 HOURS

Incident Notification:
Additional technical details, impact assessments, and mitigation measures must be provided.

AFTER THE INVESTIGATION IS COMPLETE

Final Report:
Documentation of the root cause, impact, and corrective actions implemented.

Important: The reporting timeline begins as soon as the manufacturer becomes aware of a reportable event.

What Should Manufacturers Do Now?

To comply with the new requirements, organizations should ensure that they have:

- Processes to detect and assess security incidents
- Clearly defined roles and responsibilities
- Documented reporting procedures
- Rapid access to relevant technical information
- Established incident response processes

Are You Ready for the First CRA Requirements?

OUR CRA EXPERTS CAN HELP YOU:

- ✔ Assess your organization's readiness and compliance needs
- ✔ Interpret the requirements of the Cyber Resilience Act
- ✔ Review and strengthen your existing processes
- ✔ Establish effective reporting and incident response procedures

Common Misconceptions

MANY ORGANIZATIONS INITIALLY MAKE INCORRECT ASSUMPTIONS:

"Every vulnerability must be reported."
No. Only vulnerabilities that are being actively exploited are subject to mandatory reporting.

"The reporting obligation does not apply until December 2027."
No. The reporting requirements under Article 14 of the Cyber Resilience Act take effect on September 11, 2026.

"Only manufacturers of critical products are affected."
No. The reporting obligation generally applies to all manufacturers whose products fall within the scope of the Cyber Resilience Act.

Prepare your organization today for the first mandatory CRA reporting requirements.

Talk to our CRA experts.

Contact details
TÜV Rheinland i-sec GmbH
Am Grauen Stein · 51105 Köln
Tel. 0800 806 9000 3000
service@i-sec.tuv.com

www.tuv.com/cra

TÜV Rheinland