Cyber Resilience Act – Vulnerability Reporting Obligations

Hacking Policy Council – March 2023

Several requirements of the EU Commission's proposed Cyber Resilience Act (CRA) may be construed to require vulnerabilities to be disclosed to government authorities before those vulnerabilities are mitigated:

- **Article 11.1** of the proposed CRA requires manufacturers to notify ENISA of any actively exploited vulnerabilities in products with digital elements within 24 hours. ENISA would be further required to forward these notifications to Member States' Computer Security Incident Response Teams (CSIRTs) and market surveillance authorities, and support investigations of manufacturers' potential non-compliance with the Cyber Resilience Act.[1] The 24-hour deadline increases the likelihood that the vulnerabilities will not be mitigated at the time of reporting, leading to an ongoing list of software products with unmitigated vulnerabilities that may be shared with dozens of EU government agencies.
- **Articles 13.6 and 14.4** of the proposed CRA require importers and distributors to notify market surveillance authorities immediately, rather than the manufacturer that can issue a mitigation, when they identify vulnerabilities in products with digital elements that present a significant cybersecurity risk.

Risks of premature vulnerability disclosure

When significant vulnerabilities are present, a top priority is for the manufacturer to deploy a mitigation that prevents loss or damage, and to reduce risks until that mitigation is deployed. Notably, the CRA separately requires manufacturers to address and remediate vulnerabilities without delay, so it is unnecessary to require disclosure to ENISA to drive mitigation of vulnerabilities.[2] However, the CRA proposal on vulnerability disclosure raises several concerns that may jeopardize the security of products and users:

- **Risk of alerting adversaries.** Requirements to share information about unmitigated vulnerabilities broadly with government agencies undermine cybersecurity by increasing the risk that the information will be exposed to adversaries before a mitigation is in place. Industry standards and best practices for vulnerability disclosure and incident response encourage organizations to limit the pre-mitigation disclosure of vulnerabilities only to necessary parties to reduce the likelihood of additional adversaries learning of the vulnerability and causing further harm. While the CRA requires notification of the vulnerability "with details," and not full technical specs of the vulnerability, this is enough to raise the risk of further exploitation. From the CERT Guide to coordinated vulnerability disclosure: "Mere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves."[3]
- **Risk of intelligence use.** Requirements to share unmitigated vulnerabilities broadly with government agencies increases the risk that those vulnerabilities will be used for state intelligence purposes.[4]

[1] Cyber Resilience Act (CRA), Recitals 19, 34, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.
[2] CRA, Annex I, subsection 2(2): "in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates."
[3] CERT, Guide to Coordinated Vulnerability Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInf.
[4] Microsoft, Digital Defense Report 2022, pg. 39, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022. "The increased use of zero days

ENISA recommends fostering trust by drawing a clear separation from offensive functions from digital security agencies such as ENISA, CSIRTs, and market surveillance authorities.[5]

- **International precedent.** This proposal would increase the likelihood that other governments will likewise require the disclosure of unmitigated vulnerabilities to government agencies in the absence of a cyber incident, as China has also done.[6]

- **Deterring good faith security research.** This proposal may reduce the receptivity of manufacturers to vulnerability disclosures from good faith security researchers, as the EU government would be notified of each vulnerability exploited without authorization. Article 11 and the Article 3 definition of "actively exploited vulnerability" do not distinguish between malicious criminal activity and good faith security research. This undermines the stated goals of Recital 36 in urging manufacturers to establish coordinated vulnerability disclosure policies.

Preliminary proposed solutions

To help avoid these problems, the CRA should remove reporting of unmitigated zero day vulnerabilities. The CRA should ensure timely mitigations are in place (in accordance with Annex I, subsection 2(2)) before sharing. The notification can note when the manufacturer became aware of the exploitation, so authorities can later assess if the manufacturer provided the patch without delay. We suggest that the CRA empower ENISA to publish an external catalogue of known exploited vulnerabilities, and this catalogue will identify the vulnerabilities that must be reported by manufacturers. In addition, to reduce the risk of misuse of vulnerability information, the CRA should prohibit use of the vulnerability for surveillance, military, or intelligence purposes. Finally, the definition of "actively exploited vulnerability" should distinguish between good faith security research and criminal or malicious activity.

Below are suggested modifications to Articles 11, 13, 14, and 3 to address these issues. First we provide a clean version, then a version showing edits from the CRA text.

over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority."

[5] ENISA, Developing National Vulnerability Programmes, Feb. 2023, pg. 16, https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes. "One way to do this would be to transparently inform on the separation of the government's defensive and offensive functions at institutional level when dealing with CVD."

[6] ENISA, Coordinated Vulnerability Disclosure Policies in the EU, Apr. 2022, pg. 36, https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu/@@download/fullReport.

Suggested revisions - clean

Article 11

1. During the expected lifetime of the product with digital elements, the manufacturer shall notify to ENISA any actively exploited vulnerability presenting a significant cybersecurity risk, as defined by Article 3(36), contained in the product with digital elements without undue delay and in any event within 72 hours of the following criteria being met

a) Determining that the vulnerability appears in a database of reportable known exploited vulnerabilities maintained by ENISA; and
b) Addressing and remediating the vulnerability in accordance with Annex I, subsection 2(2).

The notification shall be based on the manufacturer's coordinated vulnerability disclosure policy required under Annex I, subsection 2(5), and shall include details concerning when the manufacturer became aware that the vulnerability was actively exploited and, where applicable, any corrective or mitigating measures taken. ENISA may, without undue delay, unless for justified cybersecurity risk-related grounds such as delay to allow for timely deployment of vulnerability mitigation, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with international standards and best practices ISO/IEC 30111 and ISO/IEC 29147 and Article [Article X] of Directive [Directive XXX/XXXX (NIS2)], of Member States concerned upon receipt and inform the market surveillance authority of Member States concerned about the notified vulnerability. Manufacturers shall not be required, prior to addressing or remediating the vulnerability, to disclose technical details of a vulnerability that would enable another party to reconstruct or reverse engineer the vulnerability or malicious code to exploit the vulnerability. CSIRTs, market surveillance authorities, ENISA, and other Union and Member State agencies are prohibited from forwarding or using vulnerabilities disclosed under this Regulation to be used for offensive, military, surveillance, or intelligence-gathering purposes.

Article 11

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident reported in accordance with Article 11.2 and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

Article 13

6. Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, upon becoming aware that a vulnerability in the product with digital elements appears in the database of reportable known exploited vulnerabilities maintained by ENISA and presents a significant cybersecurity risk, importers shall immediately inform the manufacturer and ENISA to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

Article 14

4. Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, upon becoming aware that a vulnerability in the product with digital elements appears in the database of reportable known exploited vulnerabilities maintained by ENISA and presents a significant cybersecurity risk, distributors shall immediately inform the manufacturer and ENISA to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

Article 3

(39) ‘actively exploited vulnerability’ means a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner, but does not include a vulnerability for which there is reliable evidence that the exploitation was performed by an actor for purposes of good faith testing, investigation, correction, or disclosure of a security flaw or vulnerability to promote the security or safety of the system owner, computers or software, or those who use such computers or software;

Suggested revisions - showing edits

Article 11

1. During the expected lifetime of the product with digital elements, ~~T~~the manufacturer shall~~, without undue delay and in any event within 24 hours of becoming aware of it,~~ notify to ENISA any actively exploited vulnerability presenting a significant cybersecurity risk, as defined by Article 3(36), contained in the product with digital elements without undue delay and in any event within 72 hours of the following criteria being met:
    a) Determining that the vulnerability appears in a database of reportable known exploited vulnerabilities maintained by ENISA; and
    b) Addressing and remediating the vulnerability in accordance with Annex I, subsection 2(2).

The notification shall be based on the manufacturer’s coordinated vulnerability disclosure policy required under Annex I, subsection 2(5), and shall include ~~details concerning~~ when the manufacturer became aware that the vulnerability was actively exploited ~~that vulnerability~~ and, where applicable, any corrective or mitigating measures taken. ENISA may ~~shall~~, without undue delay, unless for justified cybersecurity risk-related grounds such as delay to allow for timely deployment of vulnerability mitigation, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with international standards and best practices ISO/IEC 30111 and ISO/IEC 29147 and Article [Article X] of Directive [Directive XXX/XXXX (NIS2)], of Member States concerned upon receipt and inform the market surveillance authority of Member States concerned about the notified vulnerability. Manufacturers shall not be required, prior to addressing or remediating the vulnerability, to disclose technical details of a vulnerability that would enable another party to reconstruct or reverse engineer the vulnerability or malicious code to exploit the vulnerability. CSIRTs, market surveillance authorities, ENISA, and other Union and Member State agencies are prohibited from forwarding or using vulnerabilities disclosed under this Regulation to be used for offensive, military, surveillance, or intelligence-gathering purposes.

Article 11

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident reported in accordance with Article 11.2 and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

Article 13

6. Upon identifying a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, ~~where~~ upon becoming aware that a vulnerability in the product with digital elements appears in the database of reportable known exploited vulnerabilities maintained by ENISA and presents a significant cybersecurity risk, importers shall immediately inform the manufacturer and ENISA ~~market surveillance authorities of the Member States in which they made the product with digital elements available on the market~~ to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

Article 14

4. Upon identifying a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, ~~where~~ upon becoming aware that a vulnerability in the product with digital elements was exploited in an incident involving ~~presents~~ a significant cybersecurity risk, distributors shall immediately inform the manufacturer and ENISA ~~market surveillance authorities of the Member States in which they made the product with digital elements available on the market~~ to that effect, giving details, in particular, of the non-conformity and of any corrective measures taken.

Article 3

(39) 'actively exploited vulnerability' means a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner, but does not include a vulnerability for which there is reliable evidence that the exploitation was performed by an actor for purposes of good faith testing, investigation, correction, or disclosure of a security flaw or vulnerability to promote the security or safety of the system owner, computers or software, or those who use such computers or software;

* * *

For additional information, please contact Harley Geiger, Venable LLP - HLGeiger@Venable.com