Vulnerability and Incident Reporting Procedure (ENISA Single Reporting Platform)

Document No.	CRA-IRP-001
Version	V1.0
Date of issue	2026-09-03
Prepared by	Jin Cancan
Reviewed by	Zhou Yang
Approved by	Zhou Yang
Product	Nand Flash Tracer (NFT)
Language	English (Official Version for EU Market Surveillance Authorities)

1 Purpose and legal basis

This document sets out the manufacturer's standardised procedure for reporting actively exploited vulnerabilities contained in the product and significant incidents affecting the product's security to the ENISA Single Reporting Platform (SRP) and, through it, to the Coordinated CSIRT (the "CSIRT") and ENISA, pursuant to Article 14 of Regulation (EU) 2024/2847 (the "Cyber Resilience Act" or "CRA").

Reference: Regulation (EU) 2024/2847, Article 14 (reporting obligations), Article 16 (single reporting platform), Article 13(14) (procedure to ensure continuing conformity of series production).

> *Note: The reporting obligation under Article 14 applies from 11 September 2026. This procedure takes effect on that date. It is used together with the Vulnerability Handling Process (CRA-VHP-001) and the Coordinated Vulnerability Disclosure Policy (CRA-CVD-001) as evidence of the "established vulnerability handling process" required by Annex VII, point 2(b).*

2 Scope

This procedure applies to the manufacturer, its staff, and any person formally authorised to handle vulnerabilities and security incidents on behalf of the manufacturer (the "Reporting Owner"), in respect of the following two situations:

1. The manufacturer becomes aware (including through users, researchers, the Coordinated CSIRT, ENISA, or public channels) that a vulnerability contained in the NFT product (assessed baseline version Ver 2.26.8, and later versions released during the support period) is being actively exploited;
2. The manufacturer becomes aware of a significant incident affecting the security of the NFT product.

This procedure does not apply to non-security product defects, functional bugs that do not engage the essential cybersecurity requirements, or purely commercial licence circumvention. Licence circumvention is recorded separately under the

Security Update Policy (CRA-SUP-001) and is not reported as a user-data security incident.

3 Key definitions

- **Actively exploited vulnerability**: a vulnerability that is being actually exploited by an attacker and that can compromise the essential cybersecurity requirements of the product.
- **Significant incident**: an event that has or is likely to have a negative impact on the product's ability to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions, or that has led or is likely to lead to the introduction or execution of malicious code in the product or the user's network and information systems (Article 14(5)).
- **Early warning / Vulnerability notification / Final report**: the three-stage reporting for vulnerabilities under Article 14(2).
- **Incident early warning / Incident notification / Final report**: the three-stage reporting for significant incidents under Article 14(4).

4 Reporting platform and current status

Reporting shall be made exclusively through the ENISA Single Reporting Platform (SRP).

Reference: Regulation (EU) 2024/2847, Article 14(7) and Article 16.

Current status (as of 2026-09-03, to be stated faithfully):

- The SRP is planned to become operational on 11 September 2026, the date Article 14 becomes applicable. At the time of drafting this document, the platform is not yet formally live.
- ENISA recommends that relevant parties pre-register an EU Login account so that they can log in and submit when the time comes. SRP registration and the verification of the "Assigned Representative (AR)" role may be completed when an actual report needs to be submitted, and need not be done in advance.
- **Terminology warning**: the "Assigned Representative (AR)" in the CVD context is an SRP account role, and is NOT the same as the "Authorised Representative" under Article 18 of the CRA. The two must not be confused. This manufacturer has not appointed an Authorised Representative within the meaning of Article 18 (pursuant to Article 18(1), the Authorised Representative is optional, not a mandatory obligation), and the Declaration of Conformity is issued directly by the manufacturer.

5 Determining the CSIRT endpoint for submission (Article 14(7))

Article 14(7) provides that the submission shall be made through the electronic notification endpoint of the Coordinated CSIRT of the Member State in which the

manufacturer's main establishment in the Union is located, and shall be simultaneously accessible to ENISA.

This manufacturer has no main establishment in the Union. Pursuant to Article 14(7), the Member State is determined in the following order, based on the information held by the manufacturer:

3. The Member State of the Authorised Representative acting for the largest number of the manufacturer's products;
4. The Member State of the importer placing the largest number of the manufacturer's products on the market;
5. The Member State of the distributor making available the largest number of the manufacturer's products on the Union market;
6. The Member State in which the largest number of users of the manufacturer's products are located.

As this manufacturer has not appointed an Authorised Representative and has not established importer or distributor channels, the situation falls under point (4): the first report shall be submitted through the endpoint of the Coordinated CSIRT of the Member State in which the largest number of the manufacturer's users are located; pursuant to the second subparagraph of Article 14(7), any later actively exploited vulnerability or significant incident may be submitted to the same Coordinated CSIRT first reported to.

> *The Member State with the largest number of NFT users in the Union is to be confirmed by the Reporting Owner before first submission; the Coordinated CSIRT entry-point URL is recorded once determined (determination basis: Article 14(7)).*

6 Time limits and content

6.1 Actively exploited vulnerability (Article 14(2))

Stage	Deadline	Content requirement
Early warning	Without delay and in any event within 24 hours of becoming aware	Notify the Coordinated CSIRT and ENISA simultaneously; indicate, where applicable, the Member State(s) where the product is known to have been made available
Vulnerability notification	Within 72 hours of becoming aware	General information on the product, the nature of the vulnerability and the exploitation, the corrective or mitigating measures taken and those that users may take; indicate, where applicable, the sensitivity of the information as assessed by the manufacturer
Final report	Not later than 14 days after corrective or mitigating measures are available	At least: (i) description of the vulnerability (including severity and impact); (ii) where known, information on

		the malicious actor exploiting or attempting to exploit the vulnerability; (iii) details of the security update or other corrective measures made available to users to remedy the vulnerability

6.2 Significant incident (Article 14(4))

Stage	Deadline	Content requirement
Incident early warning	Within 24 hours of becoming aware	At least whether the incident is suspected to result from unlawful or malicious behaviour; indicate, where applicable, the Member State(s) where the product is known to have been made available
Incident notification	Within 72 hours of becoming aware	General information on the nature of the incident, a preliminary assessment, the corrective or mitigating measures taken and those users may take, and an indication of the sensitivity of the information
Final report	Within 1 month of the incident notification under point (b)	At least: (i) a detailed description of the incident (including severity and impact); (ii) the type of threat or root cause that may have triggered the incident; (iii) the mitigating measures implemented and being implemented

6.3 Additional requirements

- Where necessary, the Coordinated CSIRT first receiving the notification may require an intermediate report on the status update (Article 14(6)).
- Once aware, the manufacturer shall inform affected users (all users where appropriate) of the vulnerability or incident, and where necessary of mitigating and corrective measures that users may deploy, using a structured, machine-readable format facilitating automated processing where appropriate (Article 14(8)). Where the manufacturer fails to inform users in a timely manner, the Coordinated CSIRT that has been notified may, where it considers it proportionate and necessary, provide that information to users.

7 Internal process and roles

7.1 Roles and responsibilities

- **Vulnerability Coordinator (Reporting Owner)**: a single designated person responsible for receiving and assessing external vulnerability and incident

information, deciding whether reporting is triggered, and completing the SRP submission and user notification within the time limits.

> Vulnerability Coordinator: Zhou Yang (R&D lead); backup: Jin Cancan (Testing); contact: nandflashtracer@gmail.com.

- **Technical Lead**: confirms exploitability, nature of exploitation, severity and impact, and assists in drafting the notification content.
- **Legal Representative / Approver (Zhou Yang)**: provides final confirmation of the final report.

7.2 Trigger and assessment flow

7. Intake: reports via the contact address published in the Coordinated Vulnerability Disclosure Policy (CRA-CVD-001), researcher disclosure, CSIRT/ENISA notification, or public channels (e.g. CVE, security press).
8. Registration: the Vulnerability Coordinator registers the item in the Vulnerability and Incident Log within one working day.
9. Assessment: in parallel with the Vulnerability Handling Process (CRA-VHP-001), determine whether it is an "actively exploited vulnerability" or a "significant incident".
10. Decision: once confirmed, start the reporting clock and execute the three-stage reporting per Section 6.
11. User notification: per Article 14(8), inform affected users as soon as possible, together with or after the early warning/notification.
12. Closure: after the final report is submitted, archive the report copy and the handling record (Section 8).

7.3 Time-limit control

- The Vulnerability Coordinator shall record the "time of awareness (T0)" using a unified timing tool and set reminders at 24 hours, 72 hours, and 14 days (or 1 month).
- Internal drafting shall be completed at least 4 hours before the statutory deadline to absorb uncertainty from SRP login and form filling.

8 Records and archiving

- Each report shall have a dedicated file containing: the SRP submission receipt/reference number, copies of the three-stage submissions, submission time, submitter, user notification record, and handling outcome.
- Reporting files shall be archived together with the technical documentation. The retention period follows the Document Retention Policy (CRA-RET-001): at least 10 years after the product is placed on the market or the support period, whichever is longer.
- Intermediate reports (if requested) shall be archived together.

9 Relationship with companion documents

- This procedure is the reporting execution element of the Vulnerability Handling Process (CRA-VHP-001) and provides it with SRP reporting evidence.
- The external reporting intake and the single point of contact are published uniformly by the Coordinated Vulnerability Disclosure Policy (CRA-CVD-001), and comply with Article 13(17) (the single point of contact shall allow users to choose their preferred means of communication and shall not be limited to automated tools).
- The availability of security updates is secured by the Security Update Policy (CRA-SUP-001) and is the source of point (iii) of the final report.

10 Items pending confirmation

13. Confirm, before the first formal submission, the Member State with the largest number of NFT users in the Union and the URL of its Coordinated CSIRT endpoint (Section 5).
14. Name, function and contact details of the Vulnerability Coordinator and backup (Section 7.1).
15. After the SRP goes live, complete EU Login registration and verify the actual requirements for the "Assigned Representative (AR)" role (Section 4).
16. Selection of the structured, machine-readable format for user notification (Section 6.3).

Signature record

Role	Name	Signature	Date
Prepared by	Jin Cancan		2026-09-03
Reviewed by	Zhou Yang		2026-09-03
Approved by	Zhou Yang		2026-09-03