Vulnerability Handling Process

Document No.	CRA-VHP-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 documented process for identifying, assessing, remediating, disclosing and tracking vulnerabilities throughout the product lifecycle, so as to satisfy the vulnerability handling requirements in Part II of Annex I to the CRA and Article 13(8). This process is the core evidence of the "established vulnerability handling process" required by Annex VII, point 2(b), and is used together with the Coordinated Vulnerability Disclosure Policy (CRA-CVD-001), the Security Update Policy (CRA-SUP-001), the Software Bill of Materials (CRA-SBOM-001) and the Vulnerability and Incident Reporting Procedure (CRA-IRP-001).

Reference: Regulation (EU) 2024/2847, Annex I Part II, points (1) to (8); Articles 13(2)(3)(4)(7)(8); Annex VII, point 2(b).

2 Scope

This process applies to the handling of vulnerabilities in the NFT software (assessed baseline version Ver 2.26.8, and later versions released during the support period) and in the components it contains (including third-party and open-source components). It covers the full cycle from vulnerability intake, analysis, remediation, verification, disclosure and update distribution to closure.

3 Roles and responsibilities

- **Vulnerability Coordinator**: overall owner of the process, receives external reports, organises assessment, tracks remediation progress, and interfaces with the trigger for submission under the Vulnerability and Incident Reporting Procedure (CRA-IRP-001). May be the same person as the single point of contact published under the CVD policy.

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

- **Development Lead**: implements the code fix, builds and performs internal verification.
- **Test Lead**: performs regression and security testing of the fixed version (see Test Report CRA-TR-001).

- **Legal Representative / Approver (Zhou Yang)**: approves external disclosure and the final report.

4 Vulnerability intake and registration

- External vulnerabilities enter through the contact address published in the Coordinated Vulnerability Disclosure Policy (CRA-CVD-001); internally discovered vulnerabilities are registered through development and testing activities.
- All vulnerabilities are registered in the Vulnerability and Component Log with a unique identifier (format: VUL-YYYY-NNN), recording source, date and preliminary description.
- For third-party / open-source component vulnerabilities, report promptly to the upstream maintainer pursuant to Article 13(6), and share code or documentation (in machine-readable form where appropriate) when a fix has been developed.

5 Vulnerability assessment and rating

- Severity is rated using CVSS v3.1 (Critical / High / Medium / Low), combined with an assessment of exploitability and impact in the context of a locally installed, offline professional forensic tool.
- The assessment conclusion is recorded in the log and used as the basis for remediation priority, disclosure timing, and whether Article 14 reporting is triggered.
- An "actively exploited vulnerability" or "significant incident" is immediately handed to the Vulnerability and Incident Reporting Procedure (CRA-IRP-001) to start the three-stage reporting.

6 Remediation and verification

- The remediation should eliminate the root cause at the affected component or code layer where possible; where immediate remediation is not possible, apply and record a mitigating measure.
- The fixed version must pass internal verification and the testing described in the Test Report (CRA-TR-001), confirming the vulnerability is eliminated and no new known exploitable vulnerability is introduced.
- Changes from the fix are synchronised into the Software Bill of Materials (CRA-SBOM-001) and the Cybersecurity Risk Assessment (CRA-RA-001).

7 Disclosure and update distribution

- After a security update is released, share and publicly disclose information on the remediated vulnerability pursuant to Annex I Part II, point (4): vulnerability description, information enabling users to identify affected products, impact and severity, and clear and easy-to-understand information helping users remediate.
- Where there is justified reason to consider that the public security risk outweighs the security benefit, disclosure of the remediated vulnerability may be delayed

until users have had the opportunity to apply the patch (the proviso to Part II, point (4)).
- Security updates are distributed through the channel defined in the Security Update Policy (CRA-SUP-001), ensuring timely, free-of-charge delivery (except where otherwise agreed with a business user), and, where technically feasible, separate from functionality updates.

8 Handling time limits (internal SLA)

Severity	Target remediation / mitigation	Disclosure
Critical / High	As fast as possible; if actively exploited, follow Article 14 deadlines of 24h / 72h / 14d	With the fix or together with reporting
Medium	Within the next planned security update cycle	With the security update release
Low	Included in a later version	With the security update release or archived with explanation

Note: The internal SLA above is the manufacturer's own target and does not conflict with the statutory obligations of Article 14; an actively exploited vulnerability always takes priority under Article 14 time limits.

9 Records and continuous improvement

- Pursuant to Article 13(7), systematically record relevant cybersecurity matters (including known vulnerabilities and third-party information) in a manner proportionate to their nature and risk, and update the risk assessment as appropriate.
- Review this process at least every six months, re-assessing in light of new vulnerabilities, substantial modifications, changes in the operating environment and new harmonised standards.
- The process document is kept updated throughout the support period; retention follows the Document Retention Policy (CRA-RET-001).

10 Relationship with companion documents

- Vulnerability reporting: CRA-IRP-001 (Article 14)
- External reporting intake and single point of contact: CRA-CVD-001 (Article 13(17), Annex I Part II (5)(6))
- Security update distribution: CRA-SUP-001 (Part II (2)(7)(8))
- Component inventory: CRA-SBOM-001 (Part II (1))
- Test verification: CRA-TR-001 (Part II (3))

11 Items pending confirmation

1. Names and contact details of the Vulnerability Coordinator and the Development and Test Leads (Section 3).
2. The system hosting the vulnerability log (e.g. existing project-management tool or a new register) and its backup method (Section 4).

3. The qualification and review mechanism of the person performing CVSS rating (Section 5).

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