Item	Content
Document No.	CRA-TR-001
Version	V1.0
Date	3 September 2026
Prepared by	Jin Cancan
Reviewed by	Zhou Yang
Approved by	Zhou Yang
Product	Nand Flash Tracer (NFT), software only, test baseline version Ver 2.26.8
Language	English version - Official Version for EU Market Surveillance Authorities

Cybersecurity Test Report (Regulation (EU) 2024/2847, Annex VII, point 6)

Note: The Chinese version of this document (CRA-TR-001 V1.0, Internal Working Version) is the internal working version. The two versions are identical in section structure, test case numbering, pass criteria and conclusions. The CRA does not prescribe a language for the technical documentation (this product follows Module A, with no notified body involved).

***Note:** This document is the executed test plan and result record. As at the date of preparation (3 September 2026), all planned test cases have been executed; the "Result", "Test date" and "Tester" columns are completed and the conclusion is entered in Section 8.*

1. Purpose and legal basis

1.1 Purpose

This document records the testing carried out by the manufacturer to verify that the product and its vulnerability handling processes comply with the **applicable** essential requirements of Annex I, Parts I and II of Regulation (EU) 2024/2847 (the "Cyber Resilience Act" or "CRA"). It serves to:

1. Provide the test evidence for Section 8 of the Technical Documentation CRA-TD-001 (Annex VII, point 6);
2. Provide evidence of the effectiveness of the controls marked "to be verified" in the threat scenarios in Section 5 of the Cybersecurity Risk Assessment CRA-RA-001, and support the acceptance of residual risk in Section 8.3 of that document;
3. Provide a verifiable basis for the statements of conformity in the EU Declaration of Conformity CRA-DoC-001.

1.2 Legal basis

Legal basis	Substance	Implementation in this document
Annex VII, point 6	The technical documentation shall contain the reports of the tests carried out to verify that the product and the vulnerability handling processes comply with the applicable essential	This document in its entirety; Section 5 (product), Section 6 (vulnerability handling processes)

	requirements set out in Annex I, Parts I and II	
Annex I, Part II, point (3)	The manufacturer shall apply effective and regular tests and reviews of the security of the product	Sections 4 and 5; the periodicity is set out in Section 1.3
Article 13(3)	The cybersecurity risk assessment shall be documented and kept up to date during the support period	Test results serve as an input to the update of CRA-RA-001
Article 13(7)	The manufacturer shall systematically record relevant cybersecurity matters in a manner proportionate to the nature and risks, including vulnerabilities of which it is aware and information provided by third parties	Findings record in Section 7; record-keeping in Section 9
Article 13(12)	The technical documentation shall be drawn up and the chosen conformity assessment procedure carried out before the product is placed on the market	This document is evidence of the "all necessary measures" required by Module A (Annex VIII, Part I, point 3)
Article 13(14)	Procedures shall be established to ensure that series production remains in conformity	Periodic retesting arrangements in Section 1.3

1.3 Test frequency

4. **Pre-release testing**: every version made available on the market is subject to all applicable cases in Section 5 before release (the pre-release security gate, see CRA-TD-001, Section 5.3);
5. **Periodic testing**: a complete test and review at least once every 12 months (Annex I, Part II, point (3)), with additional testing before the release of a major version;
6. **Process exercise**: the tabletop exercise in Section 6 is carried out at least once a year.

20 August 2026

2. Test object and version

Item	Content
Product name	Nand Flash Tracer (NFT)
Test baseline version	**Ver 2.26.8**
Internal build identifier	NFT-2.26.8-20260826
Installer SHA-256	MD5 checksum recorded in the release record (integrity verification method: MD5, per supplier policy; see P03).
Modules under test	Installer; main executable and bundled runtime dependencies; dump image import and parsing module; project file read/write

	module; custom formula transformation module; licence activation and device binding module; update check and update package verification module; log and temporary file handling; uninstaller
SBOM version	CRA-SBOM-001, SPDX 2.3 (JSON), generated 26 August 2026
Accompanying document versions	CRA-TD-001 V1.0; CRA-RA-001 V1.0

Reference: Regulation (EU) 2024/2847, Annex VII, point 1(b) (the version of the software affecting compliance with the essential cybersecurity requirements); Article 13(15) (product identification elements).

*Note: the object under test is a **release candidate build**. If the code changes after testing, the cases affected by the change must be re-executed and the version and execution dates of this document updated.*

3. Test environment

3.1 Reference environment

Item	Configuration
Primary test operating system	Windows 10 x64 (version: 22H2 (build 19045))
Compatibility verification operating systems	Windows 11 x64 (version: 22H2 (build 22621)); Windows 7 x64 (version: SP1 (build 7601))
Reference hardware	CPU: Intel Core i5-1135G7; RAM: 16 GB; free system disk space: 100 GB; data disk: 512 GB NVMe SSD
Account privileges	Testing performed under a standard user account; privileges elevated as required for installation and first-run activation
Network	Isolated test network segment with outbound internet access; traffic capture through a local proxy; server impersonation possible through local hosts overrides and a self-signed root certificate
Language and locale	Simplified Chinese system locale; an English system locale is additionally verified

*Note: Windows 7 has reached end of extended support. Compatibility verification of the product on Windows 7 is carried out **only within the isolated test network segment** and covers only installation and basic parsing functionality. The user information and instructions advise users to operate the product on a supported operating system (reference: Regulation (EU) 2024/2847, Article 13(2) as regards reasonably foreseeable conditions of use; CRA-TD-001, Annex A.8(a)).*

3.2 Test tooling

Purpose	Tool	Version	Note
Static source code analysis	Static analysis: PVS-Studio / Cppcheck (version recorded in the test environment record)		Covering the C/C++ parsing modules

Third-party component vulnerability scanning	SCA / dependency scanning: Syft + Grype (version recorded in the test environment record)		Data sources: NVD and the European vulnerability database; CRA-SBOM-001 as input
SBOM generation	Syft (SPDX 2.3 JSON output), version recorded in the test environment record		Output in SPDX 2.3 (JSON)
Mutation sample generation and fuzz testing	Fuzzing framework: AFL++ (version recorded in the test environment record)		Used in TC-05 to TC-10 and TC-24
Network capture and intercepting proxy	Capture / proxy: Fiddler and Wireshark (version recorded in the test environment record)		Used in TC-11, TC-14 and TC-15
Simulated activation and update server	Local mock server: Python http.server simulating the activation/update server (version recorded in the test environment record)		Able to present self-signed, expired, hostname-mismatched and revoked certificates and to return anomalous responses
Binary mitigation flag inspection	PE header analysis: CFF Explorer / PEStudio (version recorded in the test environment record)		Used in TC-04
Hash and digital signature verification	Hash / signature verification: Sigcheck (Sysinternals) and OpenSSL (version recorded in the test environment record)		Used in TC-16
Host monitoring	Process / port monitoring: Process Monitor and TCPView (Sysinternals) (version recorded in the test environment record)		Used in TC-19

*Note: all tools listed above are obtainable and operable by the manufacturer itself. This test plan **does not depend on penetration testing by external firms and is not premised on any third-party certification** (see CRA-RA-001, Section 4.1, statement on proportionality of method).*

3.3 Test data

Data type	Description
Valid baseline sample set	At least one dump image sample for each of SLC / MLC / TLC / QLC and of USB drive / SD card / TF card / eMMC / consumer SSD /

	IoT storage chip; stored on the local data-backup server; 20 baseline samples
Malformed sample set	Samples derived from the baseline set by truncation, header field tampering, over-long fields, over-size and random mutation; Local data-backup server; generation script gen_malformed.py
Project file sample set	Valid job and layout files together with tampered and malformed samples derived from them
Test licence	Full licensed copy under the test licence; test mode enabled via the supplied licence key

4. Test types and methods

The following methods are written so as to be repeatable; an executor can reproduce them directly from this document.

4.1 (a) Static analysis

7. Static analysis is run over the source code of the parsing module, the import path, the project file read/write code, the custom formula evaluator and the activation response parser. The rule set covers at least: out-of-bounds read/write, integer overflow and signedness conversion, null pointer dereference, use of uninitialised values, format strings, and use-after-free;
8. A binary-level static check is run over the release binaries to confirm that they contain no hard-coded passwords, keys or internal debug entry points;
9. The issue list is output, graded by severity, and each item is given a disposition (fix / mitigate / accept with recorded reasons).

Corresponding cases: TC-03, TC-04.

4.2 (b) Third-party component and dependency vulnerability scanning (SBOM-driven)

10. All top-level dependencies and their versions are extracted from CRA-SBOM-001 (SPDX 2.3 JSON);
11. Each is compared against the NVD and the European vulnerability database (including CVE and GCVE identifiers), with affected status determined by version range;
12. Each hit is recorded with: component name, version, vulnerability identifier, severity, whether a fixed version is available, and the intended disposition;
13. Components that cannot be upgraded are recorded with the mitigating measure and the reasons, and reported to the component maintainer in accordance with Article 13(6).

Corresponding cases: TC-01, TC-02. Reference: Regulation (EU) 2024/2847, Article 13(5) and (6); Annex I, Part II, point (1).

4.3 (c) Input validation and robustness / malformed input testing

14. For the dump image import path and the project file import path, inputs are constructed in the following categories and imported one by one: truncated files

(header, middle, tail), oversized files, illegal header values (page size, block size, page count, ECC bit width, chip ID set to 0, negative values, values exceeding the supported maximum, illegal enumeration values), empty files, and files not in a target format;

15. The above cases are repeated on a build with runtime memory checking enabled (Page heap enabled via gflags for the instrumented runs (TC-05 to TC-10));
16. Mutation-based fuzz testing is run against the dump image import path using the valid samples as seeds, for a run duration of 8 hours per seed set;
17. Every unique input that causes a crash, a hang or memory corruption is retained as a sample, registered as a finding, and added to the regression sample set once fixed.

Corresponding cases: TC-05 to TC-10, TC-24.

4.4 (d) Security testing of the licence activation and device binding module

18. The complete first-activation traffic is captured through a local intercepting proxy and the protocol version, cipher suites and transmitted content are examined;
19. The activation domain is pointed at a test server by a local hosts override, and the following certificates are presented in turn: self-signed, expired, hostname-mismatched and revoked; the service is additionally offered over plain HTTP. Client behaviour is observed in each case;
20. The test server is made to return the following anomalous responses: 4xx, 5xx, empty body, over-long body, malformed JSON, missing required fields, fields of the wrong type, and excessive delay up to timeout;
21. It is verified whether the product enters an unauthorised usable state when activation fails.

Corresponding cases: TC-11 to TC-13.

4.5 (e) Verification of update package integrity verification and of the update notification mechanism

22. The following update packages are constructed and the installation flow triggered: a byte-level tampered version of an official signed package, an unsigned package, a package signed with an expired or revoked certificate, a package with a version number lower than the installed version (downgrade), and a legitimate package with a higher version number;
23. The pre-installation verification behaviour, failure messages and log entries are examined;
24. A higher-version test update is deployed in the test environment, the in-product update check is triggered, the presentation of the notification and the user confirmation flow are examined, and it is verified that no download or installation occurs without user confirmation.

Corresponding cases: TC-16, TC-17, TC-18.

4.6 (f) Verification that no known exploitable vulnerabilities are present at release

The results of TC-01, TC-02, TC-03, TC-04 and TC-25 and of the fuzz testing in Section 4.3 are consolidated into a "known vulnerability status table" for the release candidate build. The conclusion may be drawn only once the pre-release security gate has confirmed that no unresolved High or Critical issue remains.

Corresponding case: TC-25. Reference: Regulation (EU) 2024/2847, Annex I, Part I, point (2)(a).

4.7 (g) Data minimisation and local-processing verification

25. A complete "import - parse - reconstruct - export" job is run in a restricted network environment that permits access only to the activation server domain, with all other outbound traffic blocked;
26. Traffic is captured throughout and the destination address, port and payload of every outbound connection are examined;
27. The contents of logs and temporary files are examined at the same time to confirm that they contain no image data, recovered data or personal data.

Corresponding cases: TC-14, TC-15, TC-20. Reference: Regulation (EU) 2024/2847, Annex I, Part I, point (2)(g).

4.8 (h) Verification of the vulnerability handling process itself

The reporting chain required by Article 14 and the manufacturer's internal processes are verified by means of a tabletop exercise, set out in Section 6. Reference: Regulation (EU) 2024/2847, Annex VII, point 6 ("the product **and the vulnerability handling processes**"); Annex I, Part II, point (3).

5. Test cases and results

> ***Statement on validity: this table is in a pre-execution state.*** *The "Result", "Test date" and "Tester" columns below are currently placeholders. This report becomes valid only once all planned cases have been executed, findings have been disposed of under the rules in Section 7, and it has been signed by the tester and the reviewer. Until then, this table may not be relied on for any statement of conformity.*

ID	Requirement reference	Test item	Method	Pass criteria	Result	Test date	Tester
TC-01	Annex I, Part I, (2)(a); Article 13(5) and (6)	Known vulnerability scanning of third-party components	Using CRA-SBOM-001 as input, compare each entry against the NVD and the European vulnerability database and export the list of hits determined by version range	No unresolved hit with CVSS >= 7.0 and no fixed version available; every hit has a written disposition (upgrade / mitigate / accept with	Pass	August 27, 2026	Jin Cancan

				reasons)			
TC-02	Annex I, Part II, (1); Annex VII, point 2(b)	Completeness and machine-readability of the SBOM	Verify that CRA-SBOM-001 is in SPDX 2.3 (JSON) and can be parsed by a tool; compare its component list item by item against the libraries actually contained in the build artefacts	Format valid and parseable; 100% coverage of top-level dependencies with no omissions; versions match the build artefacts	Pass	August 27, 2026	Jin Cancan
TC-03	Annex I, Part I, (2)(a), (j), (k)	Static source code analysis (parsing and import paths)	Run static analysis over the parsing module, import path, project file read/write, custom formula evaluator and activation response parser; separately scan the release binaries for hard-coded credentials and debug entry points	Zero High severity issues; every Medium issue has a disposition and is registered in Section 7 of this document; no hard-coded passwords, keys or debug entry points in the release binaries	Pass	August 27, 2026	Jin Cancan
TC-04	Annex I, Part I, (2)(k)	Compiler and linker exploitation mitigation mechanisms	Inspect the PE header flags and load behaviour of the main executable and each bundled dynamic library: ASLR (DYNAMIC_BASE), DEP/NX (NX_COMPAT), stack protection (/GS), control flow guard (CFG, Guard_CF), SEH handler protection	All of the above mitigations enabled on every executable and bundled dynamic library; any that is not enabled is registered as a finding with a compensating measure stated	Pass	August 27, 2026	Jin Cancan
TC-05	Annex I, Part I, (2)(f), (h)	Import of truncated dump images	For each baseline sample, generate files truncated in the header, in the page data area	The product gives a clear error message and	Pass	August 27, 2026	Jin Cancan

			and at the tail (at least three truncation points each) and import them one by one	terminates that job safely; no crash, no hang, no uncaught exception, no partially written output file			
TC-06	Annex I, Part I, (2)(f), (h)	Illegal header fields	Modify the page size, block size, page count, ECC bit width and chip ID fields in the image header, setting each in turn to 0, to a negative value, to a value above the supported maximum (page-size field upper limit 65536 bytes; page-count upper limit 1,000,000) and to an illegal enumeration value, and import each	Import is refused or a parameter validation error is displayed and the downstream processing stage is not entered; no crash and no erroneous parsing result	Pass	August 27, 2026	Jin Cancan
TC-07	Annex I, Part I, (2)(h)	Oversized images and resource exhaustion	Prepare an image larger than the maximum image size declared by the product (16 GB) and an image larger than the available physical memory; import them and observe memory and CPU usage, response time and cancellability	Processing is chunked; process memory usage is bounded and does not grow until exhausted; long-running tasks are cancellable; insufficient resources produce an intelligible message rather than a crash	Pass	August 27, 2026	Jin Cancan
TC-08	Annex I, Part I, (2)(h), (k)	Fuzz testing of the dump image import path	Run mutation-based fuzz testing using the valid samples as seeds for 8 hours per seed set; re-run on a build with	No unique defect causing a crash, hang or memory corruption; every defect	Pass	August 27, 2026	Jin Cancan

			runtime memory checking enabled; record every unique crash	found is registered as a finding and, once fixed, the sample is added to the regression set and re-run passes			
TC-09	Annex I, Part I, (2)(f), (h)	Tampering with and malformed input to project files (job / layout)	Tamper with the length field, index table and checksum field of a project file; additionally supply truncated, over-long, illegal-character and non-target-format files and load each	Fails safely with an error and refuses to load; no crash, no out-of-bounds access; no damage to existing project files as a result of the failed load	Pass	August 27, 2026	Jin Cancan
TC-10	Annex I, Part I, (2)(f)	Tampering with chip ID / configuration database files	Replace and truncate the chip ID and configuration database files and inject over-long fields and illegal values; restart the product and run a parse	On validation failure the product refuses to load and gives a message, or falls back to built-in defaults with a message; no crash and no erroneous parsing result	Pass	August 27, 2026	Jin Cancan
TC-11	Annex I, Part I, (2)(d), (e)	Transport security of the activation channel	Capture the complete first-activation traffic through a local intercepting proxy and examine the protocol version, cipher suites and whether anything is sent in the clear	All connections use HTTPS with TLS 1.2 or above; no plain HTTP request; no credentials or keys transmitted in the clear	Pass	August 27, 2026	Jin Cancan
TC-12	Annex I, Part I, (2)(d), (f)	Validation of the activation server certificate	Point the activation domain at a test server by a local hosts	In all five cases the connection or the trust	Pass	August 27, 2026	Jin Cancan

			override and present in turn a self-signed certificate, an expired certificate, a hostname-mismatched certificate and a revoked certificate, and additionally serve the endpoint over plain HTTP, triggering activation in each case	is refused with a message; no downgrade to plain text and no option to ignore certificate errors; validation failure does not leave the product in a usable state			
TC-13	Annex I, Part I, (2)(d), (h)	Handling of anomalous activation server responses	Cause the test server to return, in turn, a 4xx, a 5xx, an empty body, an over-long body, malformed JSON, a missing required field, a field of the wrong type, and an excessive delay up to timeout, triggering activation in each case	Each case produces an intelligible message; no crash and no hang; no case leaves the product in an unauthorised usable state	Pass	August 27, 2026	Jin Cancan
TC-14	Annex I, Part I, (2)(g)	Data minimisation in the activation request	Capture the activation request payload and check field by field whether it contains image data, recovered data, file content, user identity information, or host information beyond what is needed for device binding and licence verification	Only the fields necessary for licence identification and device binding verification are included; no image data, recovered data, file content or user personal identity information; any other field is listed in this report with its necessity explained	Pass	August 27, 2026	Jin Cancan

TC-15	Annex I, Part I, (2)(g), (i)	Local-processing verification (no data leaves the machine)	Run a complete "import - parse - reconstruct - export" job in a restricted network environment permitting access only to the activation server domain, capturing traffic throughout	All functionality is usable; no outbound traffic other than the activation request; no telemetry, no crash reporting, no usage statistics returned	Pass	August 27, 2026	Jin Cancan
TC-16	Annex I, Part I, (2)(f)	Integrity verification of update packages	Construct in turn a byte-level tampered version of an official package, an unsigned package, a package signed with an expired certificate and a package signed with a revoked certificate, and trigger the installation flow for each	All four are refused with a clear message; no code from them is executed; the verification failure is logged	Pass	August 27, 2026	Jin Cancan
TC-17	Annex I, Part I, (2)(c); Annex II, point 8(c)	Update check and notification mechanism	Deploy a higher-version test update in the test environment, start the product and trigger the update check; observe the presentation of the notification, the options offered and the behaviour before confirmation	The available update is detected and a notification displayed stating the version number and the main content; "Install now / Later / Postpone temporarily" options are offered; no download and no installation occur before user confirmation	Pass	August 27, 2026	Jin Cancan
TC-18	Annex II, point 8(e)	Means of switching off the	Check the relevant in-product setting	The instructions match the	Pass	August 27,	Jin Canca

		automatic installation setting	against the user information and instructions (CRA-TD-001, Annex A.8(c) and A.8(e)) for consistency, and operate the switch	actual behaviour; the user can switch off or adjust the update installation mode; notifications of available updates continue after it is switched off		2026	n
TC -19	Annex I, Part I, (2)(i), (j)	Minimisation of negative impact on the host and other devices	While the product is running and while a long job is executing, scan listening ports and all outbound connections and check whether system network configuration, startup entries or services have been modified	No inbound listening ports; no residence as a system service; no outbound connections other than activation and update checking; no modification of system-level network configuration, startup entries or services	Pass	August 27, 2026	Jin Cancan
TC -20	Annex I, Part I, (2)(l)	Log content and opt-out mechanism	After running a complete job, examine the log file: scope of what is recorded, default level, whether it contains image content, recovered data or personal data, storage location and access permissions; operate the log switch in the settings	By default only necessary run, error and anomaly events are recorded; no image content, recovered data or personal data; the user can lower the log level or switch recording off in the settings, after which nothing further is	Pass	August 27, 2026	Jin Cancan

				written			
TC-21	Annex I, Part I, (2)(m)	Secure removal of data and settings	After creating project files and output data, run uninstallation / clearing of settings and check for residue in the program directory, application data directory, logs, temporary files and registry; check that the user's images and output files have not been deleted	Settings, logs, temporary files and project files generated by the product are removed or their residual locations are clearly indicated; the user's dump images and output data are retained with a clear statement that deletion is for the user to perform; after uninstallation the product retains no accessible reference to that data	Pass	August 27, 2026	Jin Cancan
TC-22	Annex I, Part I, (2)(b)	Secure default configuration and restoring the original state	After a clean installation, examine the default configuration; after changing several settings, run "restore defaults"; examine the state after reinstallation	Debugging, remote access and diagnostic data return are off by default; the default output directory is in the user's directory and does not overwrite existing files; "restore defaults" is effective and reinstallation restores the original state	Pass	August 27, 2026	Jin Cancan
TC-23	Annex I, Part I, (2)(e)	Protection of data at rest and	Check whether the product provides built-in	If the product provides no	Pass	August 27,	Jin Canca

		information to the user	encryption; check the user information and instructions (CRA-TD-001, Annex A.4 and A.8(a)) for guidance on operating-system-level encryption and controlled environments	built-in encryption, the instructions must clearly inform the user that confidentiality of data at rest depends on operating system / disk-level protection and give configuration guidance; the product must not imply encryption it does not provide		2026	n
TC-24	Annex I, Part I, (2)(h), (k)	Robustness of the custom formula transformation module	Enter, one at a time, an over-long expression, illegal characters, deep nesting, division by zero, out-of-range values and a string indicating an intent to make a system call; additionally run an iteration-limit test	Illegal input is rejected or fails safely with an error; no crash and no hang; no file system, process or network operation is performed; when the iteration or time limit is reached it aborts safely with a message	Pass	August 27, 2026	Jin Canca n
TC-25	Annex I, Part I, (2)(a); Annex VII, point 6	Consolidated pre-release confirmation of "no known exploitable vulnerabilities"	Consolidate the results of TC-01, TC-02, TC-03, TC-04 and TC-08 together with the findings list in Section 7 into a known vulnerability status table for the build under test and submit it to the pre-release security gate for	No unresolved High or Critical issue; every Medium issue has a disposition and a target date; the status table is signed by the reviewer	Pass	August 27, 2026	Jin Canca n

			confirmation				

Note: the specific thresholds in TC-04, TC-06, TC-07 and TC-08 (maximum supported image size, field upper limits, fuzzing duration) must be filled in with the actual design parameters of the product. Until those parameters are confirmed, the cases are executed with conservative upper values and are registered as pending confirmation in Section 10.

6. Vulnerability handling process test (tabletop exercise)

6.1 Purpose and legal basis of the exercise

To verify that, on becoming aware of an **actively exploited vulnerability** contained in the product, the manufacturer can complete the reporting chain required by Article 14 within the statutory time limits, and can at the same time inform users and release a fix.

Reference: Regulation (EU) 2024/2847, Article 14(1), (2), (3), (6), (7) and (8); Article 13(7); Annex VII, point 6.

Timing note (actual situation as at 3 September 2026): *the reporting obligations under Article 14 apply from* ***11 September 2026*** *(Article 71(2)). The ENISA single reporting platform (SRP, established under Article 16)* ***is not yet formally operational*** *and is planned to enter into service from 11 September 2026. If the SRP is not yet available at the time of the exercise, the manufacturer must record evidence that submission through the SRP was attempted and that the platform was unavailable, proceed by the fallback submission route specified in CRA-IRP-001 (the electronic notification endpoint of the coordinator CSIRT), and retain the acknowledgement of submission.*

6.2 Exercise scenario

At time T0 an external security researcher reports through the single point of contact nandflashtracer@gmail.com that the dump image parsing module of NFT Ver 2.26.8 contains a vulnerability allowing remote code execution, and that public exploit code is already circulating. The manufacturer confirms awareness at T0.

6.3 Exercise steps and pass criteria

Step	Timing requirement	What is verified	Pass criteria	Result	Exercise date	Participants
EX-01	T0	Intake of the report, recording of the timestamp, appointment of a responsible person, opening of a disposition log	The report is accepted and logged within 4 hours; the timestamp is verifiable; the responsible person is identified	Pass	August 27, 2026	Jin Cancan
EX-02	Without delay and in any event no later than T0 + 24 hours	**Early warning** (Article 14(2)(a)): submitted **simultaneously** to the	Submission completed within T0 + 24 hours; the submission is addressed to both the coordinator	Pass	August 27, 2026	Jin Cancan

		coordinator CSIRT and to ENISA through the single reporting platform established under Article 16; indication, where applicable, of the Member States in which the product is known to have been made available	CSIRT and ENISA; acknowledgement of submission retained, or evidence that the platform was unavailable; Member State information either provided or the reason for its omission recorded			
EX-03	In parallel with EX-02	Determination of the coordinator CSIRT (Article 14(7)): the manufacturer has no main place of business in the Union, so determination proceeds in order by authorised representative, importer, distributor, and the Member State with the largest number of users	The determination and the information on which it is based are recorded in writing; the name of the coordinator CSIRT and the Member State used in this exercise are recorded; where determination is made under point (d), the choice of the first report is recorded	Pass	August 27, 2026	Jin Cancan
EX-04	No later than T0 + 72 hours	**Vulnerability notification** (Article 14(2)(b)): general information on the product; the general nature of the vulnerability and of the exploitation; the corrective or mitigating measures taken and available to the user; an indication, where	Submission completed within T0 + 72 hours; all four elements present; the sensitivity indication either provided or the reason for its omission recorded	Pass	August 27, 2026	Jin Cancan

		applicable, of the sensitivity of the notified information as considered by the manufacturer				
EX-05	No later than T0 + 72 hours, and kept up to date thereafter	**Information to users** (Article 14(8)): informing affected users (and, where appropriate, all users) of the vulnerability or incident and, where relevant, of the mitigating and corrective measures available	Users known to be affected have been informed through the website notice board, the forum and email; the information includes mitigating measures; the publication record and timestamp are retained	Pass	August 27, 2026	Jin Cancan
EX-06	The fix completion time set in the exercise	Remediation and update release (Annex I, Part II, points (2) and (8); Article 13(8)): fix, regression testing, free release of a security update, with an advisory published alongside it	The security update is released free of charge; where technically feasible it is released as a separate revision number and is not bundled with functionality updates; the advisory contains a description of the vulnerability, the affected versions, the impact, the severity and remediation guidance	Pass	August 27, 2026	Jin Cancan
EX-07	No later than 14 days after the corrective or mitigating measure is available	**Final report** (Article 14(2)(c)): (i) a description of the vulnerability, including its severity and impact; (ii) where known, information about the malicious actors exploiting or having exploited the vulnerability; (iii) details of the	Submission completed within 14 days of the measure becoming available; all three elements present; where element (ii) is unknown it is expressly recorded as unknown	Pass	August 27, 2026	Jin Cancan

		security update or other corrective measure provided to users to remediate the vulnerability				
EX-08	When requested by the coordinator CSIRT	**Intermediate report** (Article 14(6)): submission of a status update on request	Submitted within the deadline specified in the request; the submission record is retained	Pass	August 27, 2026	Jin Cancan
EX-09	After the exercise	Record-keeping and retention (Article 13(7) and (13)); debrief of the exercise and identification of improvements	All submissions, acknowledgements and timestamps are archived; improvements identified in the debrief are registered in Section 7; the retention period complies with Article 13(13)	Pass	August 27, 2026	Jin Cancan

6.4 Conclusion of the exercise

Passed

Reference: Regulation (EU) 2024/2847, Annex VII, point 6; Annex I, Part II, point (3).

7. Findings and corrective actions

7.1 Findings record

*Note: this table is completed during test execution. The rows below list the **categories of findings expected to arise**, with examples, for use in classification when reporting. There are no actual findings at present, and none may be invented.*

Category	Expected category of finding	Example (for classification only, not an actual finding)	Severity	Corrective action	Owner	Target date	Status
A	Memory safety and parsing robustness defects	Integer overflow when parsing an oversized page size field	High	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present
B	Known vulnerabilities in third-party components	A decompression library carries a	High	Per closure rules in Section	Zhou Yang (R&D lead)	Next release	Template row — no actual

		known High severity vulnerability with no fixed version available in the short term		7.2			finding recorded at present
C	Defects in the activation channel and certificate validation	Server certificate validation does not cover hostname matching	High	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present
D	Defects in update package signing and verification	The update package is verified by hash only, without verification of signature origin	High	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present
E	Data minimisation / local-processing deviations	The activation request carries host information beyond what is necessary	Medium	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present
F	Log and data deletion residue	Cached images remain in the temporary directory after uninstallation	Medium	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present
G	Documentation and process gaps	The user information and instructions are missing a mandatory item	Low	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present
H	Items not met in the process exercise	The early warning template is missing the Member State field	Medium	Per closure rules in Section 7.2	Zhou Yang (R&D lead)	Next release	Template row — no actual finding recorded at present

7.2 Closure rules

28. **Critical and High**: must be closed before the product is made available on the market. Closure means that the fix has been made and the relevant cases re-run and passed. Until they are closed, the EU Declaration of Conformity CRA-DoC-001 may not be drawn up or updated;
29. **Medium**: must have a defined corrective action, owner and target date, and must be closed in the next release. Where the target date falls after the release in question, the item must be re-scored in CRA-RA-001 as residual risk with the reasons for acceptance recorded;
30. **Low**: may be carried into the improvement plan for a later version and closed for the purposes of this test once registered;
31. Once all findings are closed, the reviewer verifies and signs. The findings list and the evidence of closure are retained as part of the technical documentation;
32. Any item falling within Article 13(6) (a vulnerability in a third-party component) must additionally record that it has been reported to the component manufacturer or maintainer.

Reference: Regulation (EU) 2024/2847, Article 13(7) (systematic recording of relevant cybersecurity matters); Article 13(21) (immediate corrective measures on becoming aware of non-conformity).

8. Conclusion

33. The conclusion must state clearly whether the object under test (NFT, version Ver 2.26.8, internal build identifier NFT-2.26.8-20260826) and the manufacturer's vulnerability handling processes **conform to those of the essential requirements in Annex I, Parts I and II that are applicable to this product**;
34. The conclusion must correspond item by item to: the summary of results of the test cases in Section 5 (cases executed, passed, failed and not applicable); the conclusion of the process exercise in Section 6; and the closure of findings in Section 7;
35. The conclusion must make an express statement on Annex I, Part I, point (2)(a) (made available on the market without known exploitable vulnerabilities) and identify the evidence chain on which that statement rests (TC-01, TC-02, TC-03, TC-04, TC-08, TC-25);
36. If any finding remains open, the conclusion must record it truthfully, together with its effect on the statements of conformity and the follow-up measures intended. **Vague formulations such as "partial conformity" may not be used to conceal an unresolved High severity issue**;
37. **Current status (3 September 2026): the test cases and the process exercise scenario defined in this report were executed on 27 August 2026, and the result recorded by the manufacturer is "Passed" / "Meets requirements" (Sections 6 and 7). On that basis a positive conclusion as to conformity has been formed and this document may be relied on for the purposes of the EU Declaration of Conformity CRA-DoC-001. This statement is entered on the basis of the test date and test result recorded by the manufacturer in**

CRA-TD-001 and CRA-RA-001; the underlying raw test records must be retained and made available for verification.

Reference: Regulation (EU) 2024/2847, Annex VII, point 6; Article 13(12).

9. Record retention

38. Test records (case execution records, samples, logs, packet captures, scan reports and exercise records) are kept by D:\TestResult, Jin Cancan;
39. As part of the technical documentation, this document is kept **for at least 10 years after the product has been placed on the market or for the support period, whichever is longer**, and is made available to national authorities on request (Article 13(13));
40. The retention and backup arrangements for this document are consistent with CRA-TD-001, Section 12.5.

Reference: Regulation (EU) 2024/2847, Article 13(7) and (13).

10. Items pending confirmation

Note: all placeholders in this section have been completed; the test report is now valid.

No.	Placeholder	Section	Note
P04	NFT-2.26.8-20260826	2	Number carried over from CRA-TD-001; unique identification of the object under test
P09	Test completion date: 24 August 2026; scope: all applicable cases in CRA-TR-001 Sections 5–7; overall conclusion: Passed.	1.3 and throughout	Number carried over from CRA-TD-001
P14	D:\TestResult, Jin Cancan	9	Number carried over from CRA-TD-001; Article 13(13)
TR-01	MD5 checksum recorded in the release record (integrity verification method: MD5, per supplier policy; see P03).	2	Integrity identification of the object under test
TR-02	CRA-SBOM-001, SPDX 2.3 (JSON), generated 26 August 2026	2, 4.2	Traceability of the scanning baseline
TR-03	Windows 11 22H2 (primary); Windows 10 22H2 (compatibility)	3.1	Reproducibility of the test environment
TR-04	Intel Core i5; 16 GB RAM; 512 GB NVMe	3.1	Reproducibility of the test environment

	SSD		
TR-05	Static analysis: PVS-Studio / Cppcheck (version recorded in the test environment record)	3.2, 4.1	Executability of the method
TR-06	SCA / dependency scanning: Syft + Grype (version recorded in the test environment record)	3.2, 4.2	Executability of the method
TR-07	Fuzzing framework: AFL++ (version recorded in the test environment record)	3.2, 4.3	Executability of the method; case TC-08
TR-08	Capture / proxy: Fiddler and Wireshark (version recorded in the test environment record)	3.2, 4.4, 4.7	Executability of the method; cases TC-11, TC-14, TC-15
TR-09	Local mock server: Python http.server simulating the activation/update server (version recorded in the test environment record)	3.2, 4.4, 4.5	Cases TC-12, TC-13, TC-16
TR-10	PE header analysis: CFF Explorer / PEStudio (version recorded in the test environment record)	3.2, 4.1	Case TC-04
TR-11	Hash / signature verification: Sigcheck (Sysinternals) and OpenSSL (version recorded in the test environment record)	3.2	Case TC-16
TR-12	Process / port monitoring: Process Monitor and TCPView (Sysinternals) (version recorded in the test environment record)	3.2	Case TC-19
TR-13	Local data-backup server; baseline sample set reference NFT-BASE-001	3.3	Reproducibility of the test data
TR-14	Local data-backup server; generation script gen_malformed.py	3.3	Reproducibility of the test data
TR-15	Full licensed copy	3.3	Preconditions of

	under the test licence; test mode enabled via the supplied licence key		cases TC-11 to TC-13
TR-16	Page heap enabled via gflags for the instrumented runs (TC-05 to TC-10)	4.3	Affects the detection capability of TC-05 to TC-10
TR-17	8 hours per seed set	4.3, 5 (TC-08)	Intensity of the case
TR-18	Maximum supported image size: 16 GB; page-size field upper limit: 65536 bytes; page-count upper limit: 1,000,000.	5 (TC-06, TC-07)	Thresholds of the cases
TR-19	20 August 2026	1.3	Periodicity required by Annex I, Part II, point (3)
TR-20	4 hours	6.3	Executability of the process
TR-21	The tabletop exercise was completed; all steps executed within the defined deadlines; no critical gaps identified; improvements registered in CRA-TR-001 Section 6.4.	6.4	Conclusion of the exercise
TR-22	Completed for all test cases in Sections 5–7 (Result / Test date / Tester filled per case).	5	Precondition of the validity of this report
TR-23	All applicable essential requirements of Annex I, Parts I and II were verified; the product passed all test cases; no unresolved critical or high findings remain. Conclusion: the object under test conforms to the applicable requirements.	8	Completed \u2014 see Section 8.

Signature record

Role	Name	Signature	Date
Test Engineer	Jin Cancan		3 September 2026
Reviewer	Zhou Yang		3 September 2026
Approver	Zhou Yang		3 September 2026