Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-13

Handling of vulnerabilities

March 2026
Version 1

MINISTERIO DE DEFENSA

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained therein, expressly rejecting any type of implied warranty that may be found related. In no event can the National Cryptologic Center be held liable for direct, indirect, incidental or extraordinary damages arising from the use of the information and software indicated even when it is warned of such possibility.

LEGAL NOTICE

It is strictly prohibited, without the written authorization of the National Cryptologic Center, under the sanctions established by law, the partial or total reproduction of this document by any means or procedure, including reprography and computer processing, and the distribution of copies thereof by public rent or loan.

COURTESY TRANSLATION NOTICE

This document is provided solely as a courtesy translation. This translation has been generated using automated tools with minimal human supervision. In the event of any discrepancy, ambiguity, or conflict between this translation and the original Spanish version, the original Spanish version text shall prevail and shall be deemed the only official, authoritative, and legally binding version.

VERSION CONTROL

Version	Comments
1.0	Initial version

INDEX

1. INTRODUCTION

1. This document defines the procedures and processes through which the National Certification Authority (**NCCA**) performs its role in the management of vulnerabilities affecting certified ICT products, services and processes, in accordance with **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (hereinafter the CSA) [CSA**], **Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down detailed rules for the application of Regulation (EU) 2019/881 as regards the adoption of the European cybersecurity certification scheme based on the Common Criteria (EUCC), and the Vulnerability Management and Disclosure Guidelines [VULMD].**

2. PREPARATORY STEPS

2. The Head of the **NCCA** Unit (**JAN**) shall publish on the authority's official website (**WNCCA**) information and guidance on how to report vulnerabilities by email, including the detailed procedure for their processing.

3. Forms (or templates) with instructions for completing them will be made available. The form shall specify the mandatory information to be completed.

3. VULNERABILITY MANAGEMENT PROCEDURES

4. The **NCCA** does not directly manage vulnerabilities but shall perform monitoring and coordination functions, ensuring that vulnerabilities that may affect certified products are adequately addressed by the responsible actors, in particular the **certificate holder** and the Certification Body (**CB**)

3.1 RECEIVING VULNERABILITY REPORTS

5. In the **EUCC** scheme, primary responsibility lies with the certificate holder, who shall record the information received and carry out a vulnerability impact assessment in accordance with the requirements of the scheme.

6. The **NCCA** shall not act as the primary point for receiving vulnerability reports; it shall be informed of certain aspects of the vulnerability management process affecting certified products, in the exercise of its supervisory functions.

7. The **NCCA** may be informed of vulnerabilities, in the following situations:

   - When the **CB** informs the **NCCA** of a case that may affect the status of the certificate, arising from the validation or assessment of the vulnerability impact analysis carried out by the certificate holder
   - When the **NCCA** is requested to extend the deadline for vulnerability handling.

8. Any communication concerning vulnerabilities of certified ICT products, services or processes may be addressed to **NCCA** via encrypted email using the PGP key available on the official website of the authority **(WNCCA)**.

3.2 REGISTRATION AND MONITORING

9. For each form or vulnerability report received, a record will be created or updated in the Information System of the National Cybersecurity Certification Authority **(SGA)**. The designated **NCCA** technical staff (**TA**) shall record all relevant details, including the date of receipt, the certificate holder, origin of the report, the **CB** responsible for certification, identification of the affected certified product or service (with reference to the certificate) and a description of the vulnerability.

10. This comprehensive register supports transparency, traceability and subsequent reviews, including peer assessments referred to in Article 45 of the **[EUCC]**.

3.3 DECISION ON DEADLINE EXTENSIONS AND COORDINATION AT EUROPEAN LEVEL

11. **The holder of the EUCC** certificate shall be responsible for carrying out a vulnerability impact assessment in accordance with the timelines set out in the **EUCC** scheme and the corresponding reference table **[VULMD].**

12. In certain cases**,** the certificate holder may request an extension of the deadline for carrying out the impact analysis or implementing corrective measures related to a vulnerability.

13. In accordance with the **EUCC** scheme and **[VULMD]**, there are certain situations in which the certificate holder may submit an application for a deadline extension.

14. Where **the certificate holder** considers it necessary to extend the deadline for completing the vulnerability impact assessment, they shall submit an application for extension to the **NCCA**. This request shall be submitted through the communication channel set out in Section *3.1* and shall be received by the **NCCA (JAN)**. Upon receipt of the application, the **NCCA** shall issue an **acknowledgment of receipt of the notification**.

15. The application must be submitted at least thirty days before the end of the applicable deadline and include:

    - the current version of the vulnerability impact assessment report, even if it is not finalized;
    - the technical justification of the requested extension.

16. The **JAN** shall assign a **TA** for registration in an existing file in the **SGA** and for the technical evaluation of the extension request. Such assessment shall be carried out considering the potential impact on users or on society and the impact on trust in the certification process. The decision on the extension shall be reviewed and approved by **JAN**

17. If the holder of the certificate does not receive a response to the request for extension within thirty days of the acknowledgement of receipt, the application shall be deemed accepted by the **NCCA**.

18. The **JAN** should inform the European Cybersecurity Certification Group **(ECCG)** in a timely manner on the extensions granted, with the aim of promoting the harmonization of the vulnerability management process between Member States.

19. Where the deadline for the preparation of the vulnerability impact assessment is established by mutual agreement between the **CB** and the holder of the **EUCC** certificate, the **NCCA** shall be informed. This information shall be recorded by the **TA** in the **SGA**. The maximum recommended period for such mutual agreements should not exceed 180 days.

3.4 MONITORING DECISIONS

20. The **NCCA** shall exercise oversight functions over decisions taken by **CBs** where, upon receipt of the vulnerability impact assessment report, the **CB** is required to perform the necessary validations in order to determine whether such vulnerability may affect the conformity of the product with its certificate.

21. As a result of this assessment, the **CB** may take appropriate decisions regarding the status of the certificate.

22. The **NCCA** shall be informed by the **CB**, through the channel set out in Section 3.1, of the validations carried out and the decisions taken where these may have an impact on the status of the certificate or on confidence in the certification scheme.

23. The information received shall be managed by the **JAN** and recorded in the **SGA** by the designated **TA**, in order to enable the case follow-up in the framework of the supervisory activities of the authority, in accordance with the procedure «*ANCC-PO-07, monitoring compliance*' and, where appropriate, the procedure '*ANCC-PO-11, peer review of the NCCA*.

24. In the exercise of its supervisory duties, the **NCCA** may request additional information from the **CB** or the holder of the certificate, where it considers it necessary to verify the correct application of the requirements of the **EUCC** scheme.

3.5 COORDINATION WITH CSIRT AND EXCHANGE OF INFORMATION

25. The **NCCA** shall, where necessary and as required by the regulatory framework, coordinate with other actors. In general, the national **CSIRT** (or other competent incident response team) shall only be informed or involved when the nature of the vulnerability requires immediate incident response or public safety protection measures beyond the scope of certification. For example, if a vulnerability is being actively exploited and poses a significant risk to users or critical systems, the **JAN** may notify the relevant national **reference CSIRTs** for broader containment or warning measures. In other cases, regular vulnerability management under certification may be developed without direct **CSIRT** intervention.

3.6 DOCUMENTATION AND REPORT

26. All actions taken, decisions taken and communications issued or received in the context of vulnerability management shall be documented comprehensively. The **NCCA** shall use these records to update its internal procedures and to feed future assessments (e.g. risk assessments for surveillance or recertification activities).

27. The **NCCA** shall produce statistics and summary information on recorded vulnerabilities, which shall form part of its annual reporting obligations under the **CSA**. In accordance with the *ANCC-PO-01 Annual Report*, the **NCCA** shall include in its annual report to **ENISA** and the **ECCG** aggregated data on vulnerabilities detected in certified products and the measures taken (e.g. number of reports received, number of certificates suspended or withdrawn due to vulnerabilities, etc.), as well as the main coordination actions carried out. This ensures transparency at European level and enables the European cybersecurity certification framework to benefit from the experience gained. In addition, the complete dossiers shall be available for the peer assessment of the **NCCA** (Article 45 of the [**EUCC]**) to demonstrate that the vulnerability management process of

the **NCCA** is robust and fully compliant with the **CSA**, the **EUCC** scheme and the **ENISA** and **ECCG** guidelines on vulnerability management and disclosure.

4. REFERENCES

ACCCB	Accreditation of certification bodies for EUCC (https://certification.enisa.europa.eu/publications/accreditation-cbs-eucc_en)
ACCITSEF	Accreditation of ITSEF for EUCC (https://certification.enisa.europa.eu/publications/accreditation-itsefs-eucc_en)
AUTH	Authorisation of certification bodies and ITSEF for the EUCC scheme (https://certification.enisa.europa.eu/publications/eucc-guidelines-authorisation-cabs_en)
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies, and repealing Regulation (EU) No 526/2013 (http://data.europa.eu/eli/reg/2019/881/oj)
CSA-E1	Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (http://data.europa.eu/eli/reg/2025/37/oj)
EUCC	Implementing Regulation (EU) 2024/482 of the 31 January 2024 Commission laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European criteria-based cybersecurity certification scheme common (http://data.europa.eu/eli/reg_impl/2024/482/oj)
LPAC	Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (https://www.boe.es/eli/es/l/2015/10/01/39/con)
NOTIF	Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 laying down the circumstances, formats and procedures for notification in accordance with Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies (http://data.europa.eu/eli/reg_impl/2024/3143/oj)
VULMD	Guidelines on Vulnerability Management and Disclosure (https://certification.enisa.europa.eu/publications/eucc-guidelines-vulnerability-management-and-disclosure-and-eccg-opinion_en)

5. ACRONYMS

NCCA	National Cybersecurity Certification Authority
CCN	National Cryptologic Center
EC	European Commission
CSIRT	Computer Security Incident Response Teams
ENAC	National Accreditation Body
ENISA	European Union Agency for Cybersecurity
EUCC	European cybersecurity certification scheme based on common criteria
ECCG	European Cybersecurity Certification Group
ITSEF	Information Technology Security Evaluation Facility
JAN	Head of the NCCA unit
CB	Certification Body
CAB	Conformity assessment body
CSA	Cybersecurity Regulations
SED	Secretary of State Director of the CCN
SGA	Information System of the National Cybersecurity Certification Authority
TA	Technical staff attached to the NCCA
ICT	Information and Communication Technologies
EU	European Union
VPA	Voluntary periodic audits
WNCCA	Website of the National Cybersecurity Certification Authority