EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME GUIDELINES ON VULNERABILITY MANAGEMENT AND DISCLOSURE

Version 1.1, January 2025

DOCUMENT HISTORY

Date	Version	Modification	Comment
October 2023	0.1		First draft
March 2024	0.95	Update after TG review	First version submitted to the ECCG
June 2024	1.0.5	Conversion of the document into guidelines	Second version submitted to the ECCG
December 2024	1.0.11	Integration of EC final comments	Version endorsed by the ECCG
January 2025	1.1	Editorial review	Version for publication

LEGAL NOTICE

LEGAL NOTICE

This publication is a guidelines document supporting Commission Implementing Regulation (EU) 2024/482.

This document is established under the responsibility of the European Cybersecurity Certification Group (ECCG) and may be updated whenever needed to reflect the developments and best practices in the field of the vulnerability management and disclosure..

This document should be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes, and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf for the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

CONTACT

Feedback or questions related to this document can be sent via the European Union Cybersecurity Certification website (https://certification.enisa.europa.eu/index_en)

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Objective of the document

This guidelines document supporting the EUCC scheme provides guidance for the holder of the EUCC certificate and the IT Security Evaluation Facilities (ITSEF) on how to apply the rules related to vulnerability handling and disclosure of the Implementing Regulation (EU) 2024/482 establishing the EUCC scheme. It also includes guidance for the CB (certification body), for the NCCAs (National Cybersecurity Certification Authority) and the CSIRT (Computer Security Incident Response Team) designated in the Member State as coordinator for the purposes of coordinated vulnerability disclosure process.

This document is intended to be updated to further cover the specific case of composite evaluations, as well as to take benefit of other schemes established under the CSA, and to ensure consistency with applicable EU legislation, in particular the Cyber Resilience Act.

1.2 References

ID	Title of document
CSA	Regulation (EU) 2019/881 of The European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
EUCC scheme (EUCC)	Commission Implementing Regulation (EU) 2024/482 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
NIS 2	Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
ISO/IEC 15408-1:2022	Evaluation criteria for IT security Part 1: Introduction and general model
ISO/IEC 15408-2:2022	Evaluation criteria for IT security Part 2: Security functional components
ISO/IEC 15408-3:2022	Evaluation criteria for IT security Part 3: Security assurance components
ISO/IEC 15408-4:2022	Evaluation criteria for IT security Part 4: Framework for the specification of evaluation methods and activities
ISO/IEC 15408-5:2022	Evaluation criteria for IT security Part 5: Pre-defined packages of security requirements
ISO/IEC 18045:2022	Evaluation criteria for IT security Methodology for IT security evaluation
ISO/IEC 29147:2018	Vulnerability disclosure
ISO/IEC 30111:2019	Vulnerability Handling processes
TLP	Traffic Light Protocol : https://www.first.org/tlp/
RFC 9116	A File Format to Aid in Security Vulnerability Disclosure
ISO/IEC 17065:2012	Conformity assessment Requirements for bodies certifying products, processes and services

2 SCOPE

EUCC Article 32 – Scope of vulnerability management

The scope of the current document corresponds to the ICT products for which an EUCC certificate was issued and for which there are subsequently detected vulnerabilities. The chapters below contain guidance on the process to be followed in such cases.

Note: Vulnerabilities that do not impact an EUCC certificate are outside the scope of this guidance.

3 VULNERABILITY MANAGEMENT PROCEDURE

EUCC Article 33(1) – Vulnerability management procedures

As stated in Article 33(1) of the EUCC scheme, the holders of EUCC certificates must follow the vulnerability management rules as set in the EUCC scheme supplemented by ISO/IEC 30111:2019 Information technology - Security techniques - Vulnerability handling processes pursuant to EUCC.

It is recommended to follow the general steps of ISO/IEC 30111:2019 as follows:

- preparation,
- receipt,
- verification,
- remediation development,
- release,
- post release,

with the specific application rules for the EUCC scheme. In addition to the requirements set out in the EUCC scheme (see 3.1. below), it is recommended that the holder of the EU certificate makes available to the relevant stakeholders its vulnerability management procedure and usage of best practices of how it follows the current guidance.

3.1 Preparation

EUCC Article 33(1) – Vulnerability management procedures
CSA Article 55(1)(c) – Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes

As stated in Article 33(2) of the EUCC scheme," *the holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers."*

Such information is required to be made public in accordance with Article 55(1)(c) of the CSA. Such methods may contain (the list is not exhaustive): bug-bounty programs, dark web monitoring, following vulnerability disclosure platforms etc.

As stated in Article 55(1)(c) of the CSA, the contact information of the holder of the EUCC certificate - electronic contact information - and the method of sending, such as the method of encryption, must be made public.

A recommended option is to use the security.txt file according to RFC 9116 to provide the methods for receiving vulnerability information.

3.2 Receipt

EUCC Article 27(1)(a) Monitoring activities by the holder of the certificate *EUCC Article 33(3), (4) and (5) – Vulnerability management procedures* *EUCC Article 35(3) – Vulnerability impact analysis report*
CSA Article 55(1)(c) and (d), Article 55(2) – Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes *CSA Article 56(8) – Cybersecurity certification*

The following cases where:

- the holder of the EUCC certificate receives vulnerability information according to Article 55(1)(c) of the CSA, or receives information on a potential vulnerability from the CB that issued the certificate;

- there is a new publicly disclosed vulnerability on the referenced online repositories according to Article 55(1)(d) of the CSA which is found also relevant for the EUCC certified product;
- the holder of the EUCC certificate finds out a potential related vulnerability to its ICT certified product in any other way,

can be considered to correspond to the cases according to Article 33(3) where a holder of an EUCC certificate detects or receives information about a potential vulnerability affecting a certified ICT product, and shall record it and carry out a vulnerability impact analysis.

It is recommended to keep a record of received information that leads to the next steps of vulnerability handling. This is for audit and accountability purposes, also for supervising activities of the NCCA.

In line with the EUCC scheme, a potential vulnerability can be understood as a reported, but not yet verified vulnerability. Its potential nature means that it needs to be verified, whether the reported misbehaviour related to security functionality of the product violates the implicit or explicit security policy in that product.

The EUCC scheme requires at this stage that a vulnerability impact analysis must be completed, to see if the potential vulnerability is applicable. In ISO/IEC 30111:2019, this is referred to as initial investigation.

The vulnerability impact analysis should be started without undue delay and be performed within a reasonable time. During the vulnerability impact analysis, to enquire whether the vulnerability has a likely impact on the conformity of the ICT product with its certificate, the holder of the certificate should investigate whether the potential vulnerability:

1) can be qualified as “previously undetected”, meaning it is previously unknown;
2) concerns the security of the ICT product;
3) may have an impact on the compliance with the requirements related to the certification.

If any of the above conditions are not met and the vulnerability has no likely impact on the conformity of the ICT product with its certificate, the process should stop with the recording of the information identified below. The vulnerability impact analysis report should then not be produced, only the record should be kept about the vulnerability impact analysis.

The above list also implies the process exits, which are the same as those mentioned in ISO/IEC 30111:2019:

- Duplicate entry: report about a potential vulnerability, which is already received, meaning that the report is about a previously already detected issue. Note: If information about a potential vulnerability is reported or detected redundantly, the additional reports or detections can be added to the original record of information as a further reference.
- No security: Report has no security implications or it has, but these cannot be exploited within the scope of the certificate.

In addition, to prevent being overwhelmed by reports from having to respond to multiple false notifications, the holder of the EUCC certificate should assess the trustworthiness of the sources, based on prior records and available evidence (eg. Multiple false notifications). The sources that the EUCC certifiation holder decided to disregard in the future should be recorded together with the reasoning, and in case of a request from the CB according to EUCC Article 33(5), these records should be also transmitted to the CB.

If the above conditions are all met, the next step is to ascertain whether the potential vulnerability might impact a composite product, and according to EUCC Article 33(4), the holder of the EUCC certificate shall inform the holder of dependent EUCC certificates about potential vulnerability.This should include at least least all the the known holder(s).

For all potential vulnerabilities the recorded information should contain the following elements:

- Identification of the potentially affected certified product, also including the identification of the certificate,
- source of information,
- summary of information received,
- in case of a process exit before the full process is completed, reason of the exit,
- indication whether the potential vulnerability might impact a composite product.

Where the information received is to be sanitised, it is recommended to remove the exploitation details from the information received, and to summarize the content in a way that allows identification of the received information.

In addition, following EUCC requirements apply:

- According to Article 33(5): In response to a reasonable request by the certification body that issued the certificate, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to that certification body;
- According to Article 35(3): Information pertaining to possible means of exploitation of the vulnerability shall be handled in accordance with appropriate security measures to protect its confidentiality and ensure, where necessary, its limited distribution.

3.3 Verification

EUCC Article 7(2) – Evaluation criteria and methods for ICT products
EUCC Article 34(1) and (2) – Vulnerability analysis
EUCC Annex IV.4 – Patch management

After the information referred to in the above chapter has been recorded, the vulnerability impact analysis starts. The timeline starts when the vulnerability impact analysis of received information (as defined in chapter 3.2 by the vendor's Product Security Incident Response team, or its equivalent), has confirmed that the vulnerability may have a possible impact on the conformity of the ICT product related to the certification.

In line with the EUCC scheme, holders of EUCC certificates are obliged to inform the CB about the vulnerability impact analysis and perform other support (e.g. immediate remediation, warnings etc.) without undue delay, when the vulnerability is proven to be already exploited and this is publicly known.

The timeframe maximum to conduct the vulnerability impact analysis should be as follows:

Attack potential values[1]	Attack potential for attackers	Severity rating for remediation	CSA Assurance Level		Meets assurance components:	Failure of components:
			Substantial (<VAN.3)	High (>= VAN.3)		
0-9	Basic	**Critical**	60 CD*	60 CD*	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10 to 13	Enhanced-Basic	**High**	Mutual Agreement	90 CD*	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	**Medium**	Timing up to the certificate holder	90 CD* (VAN.4 and VAN.5) Mutual Agreement** (VAN.3)	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	**Low**	Timing up to the certificate holder	90 CD* (VAN.5) Mutual Agreement** (VAN.4) Timing up to the certificate holder (VAN.3)	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	**N.A.**	Timing up to the certificate holder	Timing up to the certificate holder	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Table 1: Guidance on maximum timeframes for the vulnerability impact analysis

CD=Calendar Days

For vulnerabilities under active exploitation, time to analyse should be reduced to the minimum possible and patches should be made available without undue delay. "Under active exploitation" means that there is a vulnerability for which there is reliable evidence that execution of malicious code was performed on a system without permission of the system owner. Within the scope of the current document, the actively exploited vulnerabilities are those vulnerabilities, where

[1] The table was designed based on ISO/IEC 18045:2022 section B6 Calculating attack potential

this is indicated in the European vulnerability database[2], or where the CB or the NCCA have such evidence, and have informed the holder of the EUCC certificate about this. If the holder of the EUCC certificate receives information about an active exploitation of a vulnerabilty to its ICT certified product by any other way, the holder should prioritise their analysis and inform the CB.

Also note: There is a difference between patching and recertification. Priority should be given to the correction of the vulnerability, and then to the renewal of the certification. This can be done especially with the application of the patch management approach of EUCC Annex IV.

If there is a potential vulnerability that puts at risk the security of an ICT product and impact its certification compliance, it is essential to carry out an attack potential calculation. Yet, as per ISO/IEC 18045:2022 Vulnerability Assessment, it remains a requirement to check if the vulnerability can be exploited at the intended VAN level. To understand the significance and need for attack potential calculation, see Annex B of ISO/IEC 18045:2022.

The timeframes indicated above are the recommended maximum limits, except where the timing is up to the certificate holder, due to the risk assessment above. If the vulnerability impact analysis report is available before the indicated time limit, especially in case of Critical and High severity, the report should be shared as soon as it is available.

The times indicated in the above table with an asterisk (*) may be extended with the approval of the related NCCA.

The times indicated in the above table with a double asterisk (**) should be 90 days in case there is no mutual agreement.

The extension should be possible to any agreed number of times if 30 days before the end of the timeline the holder of the EU certificate delivers the actual version of the impact analysis report that could not be finalised yet, together with the justification for the extension to the CB and NCCA. The NCCA may approve another 60/90 days as an extension to the time of the impact analysis, the NCCA should consider the impact on the society and the trustworthiness in the decision process. The NCCA should acknowledge the receipt of the extension request. If the holder of the certificate does not receive an answer to the extension request within 30 days, other than the acknowledgement of receipt, the extension request should be considered as accepted by the NCCA.

The NCCA should inform in due time the ECCG about extensions in order to harmonise the vulnerability management process.

The mutual agreement in the above table means the agreement of the CB and the holder of the EUCC certificate about the timeline of creating the vulnerability impact analysis. These mutual agreements are indicated in the above table related to cases where the result of the attack potential calculation is close to the assurance component included in the certificate. The mutual agreement should be recorded. The NCCA should be informed about the mutual agreement. Recommended maximum timeframe of the mutual agreement should be no more than 180 days.

In the case where timing is up to certificate holder, the attack potential exceeds the VAN level of the certificate already significantly. These cases should be handled as for all other residual vulnerabilities (e.g. recorded, observed and looked at from time to time).

The CB (or in case of CB monitoring, the NCCA) should validate the result of the attack potential calculation at the validation of the vulnerability impact analysis report, or when the result of the attack potential calculation is doubtful. If the vulnerability impact analysis procedure is not continued based on the attack potential calculation, the holder of the EUCC certificate should inform the CB, and the information should contain the details of the attack potential calculation. Where applicable, the relevant technical domain documents should be used, e.g. EUCC state-of-the-art document ‘Application of Attack Potential to Smartcards’.

Where the holder of the certificate received information from external resources, the holder of the certificate may seek additional information, before the calculation is concluded.

Based on the attack potential calculation there could be two possible outcomes related to the vulnerability impact analysis, and the exploitable vulnerability is either:

a) within the boundaries of the AVA_VAN level stated by the certificate: the holder of the certificate should then further analyse the vulnerability, e.g. by creating an exploit that verifies the exploitability of the vulnerability;
b) beyond the boundaries of the AVA_VAN level stated by the certificate: the holder of the EUCC certificate should record it and retain the analysis for 5 years.

Where the vulnerability impact analysis confirms the existence and relevance of the vulnerability regarding the likely impact on the conformity of the ICT product with its certificate, an impact analysis report must be created related to the issue within the above indicated timeline in line with EUCC Article 35.

At this point, if the potential vulnerability might impact a composite certified product, the holder of the EUCC certificate should inform all the known holder(s) of dependent EUCC certificates about the potential vulnerability.

[2] The European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 of the European Parliament and of the Council.

Where the vulnerability impact analysis demonstrates the absence of a vulnerability, the holder of the certificate should record and retain the analysis for at least 5 years.

3.4 Impact Analysis Report

EUCC Article 14(1-3) – Withdrawal of an EUCC certificate *EUCC Article 29(1-4) – Consequences of non-compliance by the holder of the certificate* *EUCC Article 35(1-5) – Vulnerability analysis report*
CSA Article 56(8) – Cybersecurity certification *CSA Article 63(1-2) – Right to lodge a complaint*

In the case the exploitability of the vulnerability is confirmed and applies to the certified ICT product, the following should apply.

If the information contains details about the possible exploit(s) of the vulnerability: it should carry one of the below mentioned ways of classification to ensure the relevant levels of protection:

- the appropriate Traffic Light Protocol (TLP) classification, applied in accordance with the standard rules defined in https://www.first.org/tlp/;
- or, alternatively, classification of information, data, and material as set out in the EUCC state-of-the-art document 'Minimum Site Security Requirements'.

In line with EUCC Article 35(3), the information including details about possible exploits must be handled and transferred to the CB or the NCCA in accordance with appropriate security measures to protect its confidentiality, availability and integrity to ensure, where necessary, its limited distribution. ISO/IEC 29147:2018 lists TLS, S/MIME and OpenPGP as typical security mechanisms which may be considered.

The limited distribution should include the CB, the NCCA (where applicable), the ITSEF and the holder of the EUCC certificate. If any of these parties needs to share the impact analysis report further, they should remove the description of possible means of exploitation of the vulnerability.

In line with EUCC Article 43, all stakeholders (CB, ITSEF, NCCA, CSIRT) must also handle the information shared with them in accordance with appropriate security measures to protect its confidentiality, availability and integrity and ensure, where necessary, its limited distribution.

In line with EUCC Article 35(4) scheme, the vulnerability impact analysis report must be sent without undue delay to the CB or the NCCA in accordance with CSA Article 56(8). The CB or the NCCA may request additional clarifications.

In line with Article 35(6) EUCC, where the vulnerability impact analysis report indicates that the vulnerability cannot be remediated, the certificate must be withdrawn in accordance with Article 14 of the EUCC.

The vulnerability impact analysis report should be stored, and the relevant documentation kept for at least five years by all parties who received the analysis.

3.5 Remediation Development

EUCC Article 13 – Review of an EUCC certificate *EUCC Article 36 – Vulnerability remediation*

If the certified ICT product includes a patch management mechanism, as defined in EUCC Annex IV.4 that was assessed within its certification, the associated conditions must apply.

Where the certified ICT product does not include such a patch management mechanism, the review process described in EUCC Annex IV.3 must be applied to verify the correctness of the changes made to cover the vulnerability, and to reissue any necessary updated certificate. No change should be implemented to the certified product without a certified patch management before its re-certification. However, for vulnerabilities that are under active exploitation, priority should be given to mitigating risks.

In addition, following EUCC requirements apply according to its Article 36:

- the holder of an EUCC certificate shall submit a proposal for an appropriate remedial action to the CB leading to the necessary changes to the ICT product;
- the CB shall review the certificate in accordance with EUCC Article 13.

3.6 Release and post release

CSA Article 55(1)(d) – Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes

Where remediation and associated changes to the ICT product have been declared apt for deployment, by the CB, the holder of the certificate should directly proceed to the deployment of remediation and associated changes, or proceed to their release in accordance with the requirements of CSA Article 55(1)(d). All remediation and associated changes to the security lifecycle should be implemented urgently and efficiently.

The security lifecycle of the ICT product should in addition be updated, meaning that if the development process needs to be updated to mitigate reoccurrence of the vulnerabilities, or the type of vulnerabilities, it should be done.

4 VULNERABILITY DISCLOSURE

EUCC Article 37(1-2) – Information shared with the national cybersecurity certification authority *EUCC Article 38(1-2) – Cooperation with other national cybersecurity certification authorities* *EUCC Article 39 – Publication of the vulnerability*
CSA Article 55(1)(d) – Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes *CSA Article 58(7)(h) – National cybersecurity certification authorities*

The holders of EUCC certificates should use the following standard for the general guidelines related to vulnerability disclosure:

- ISO/IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure.

In addition to the general disclosure guidance above, once a strategy to correct the vulnerability has been defined by the holder of the certificate, or as soon as the decision was taken that the vulnerability could not be mitigated, information related to the confirmed vulnerability must be disclosed to the NCCA by the CB, including updates and progresses of the strategy in accordance with CSA Article 56(8) and EUCC Article 37.

According to EUCC Article 37(2), the information must not contain details about the possible exploit of the vulnerability. It must contain the necessary elements for the NCCA to understand the nature and impact of the vulnerability on the compliance requirements related to the product's certification, the changes to be brought to the product, and where applicable, information by the CB on the broader applicability of the vulnerability to other certified products according to EUCC Article 37(1). The latter should take into account the extra time provided to certification of the composite product.

The NCCA must in accordance with CSA Article 58(7)(h) and EUCC Article 38 share this information with ENISA and other NCCAs which may also decide to further analyse the problem or, after informing the EUCC certificates holder of the ICT product about the information exchange, ask the related CBs to analyse whether further certified products are affected. This information exchange must be done in a secure and confidential manner in line with EUCC Article 43. The information should be signed and encrypted.

In addition, upon withdrawal of a certificate, the holder of the EUCC certificate shall disclose and register any publicly known and remediated vulnerability in the ICT product on the European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 of the European Parliament and of the Council or other online repositories referred to in CSA Article 55(1)(d).

5 BACKGROUND INFORMATION

The EUCC Scheme vulnerability handling and disclosure processes are based on ISO/IEC 30111:2019 and ISO/IEC 29147:2018. However, as these standards do not contain any assurance on whether the developed and deployed remediation does not introduce new vulnerabilities, and do not define any tasks for a third-party assessment body and its methodology, additional information was provided into this guidance document to cover these gaps.

The following figure gives an overview of the process:

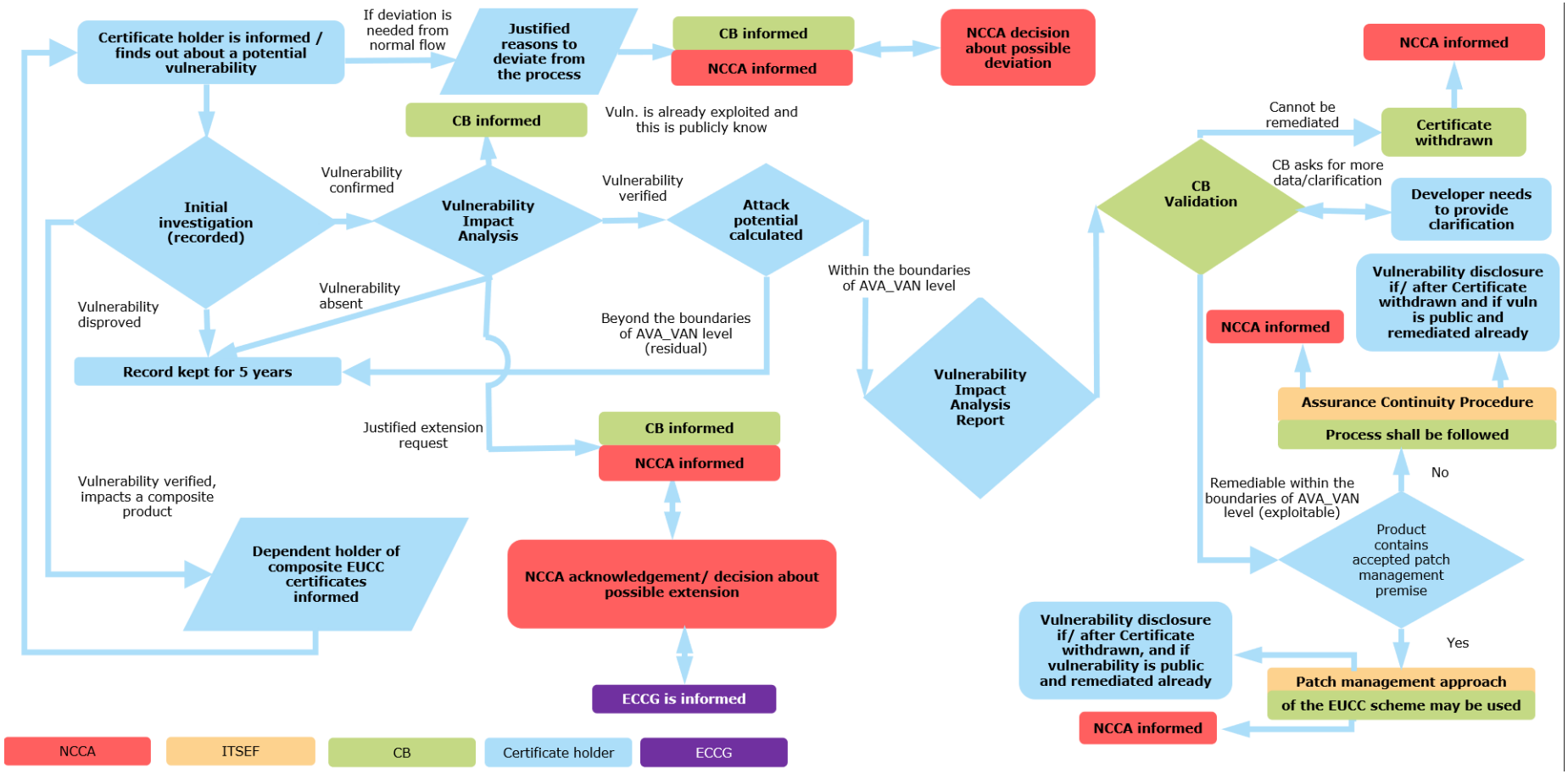

Figure 1: Recommended Vulnerability handling and disclosure processes limited to those of certification relevance.

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu