



**PREMIER  
MINISTRE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général de la défense  
et de la sécurité nationale**

Agence nationale de la sécurité des  
systèmes d'information

Paris, le 04/03/2026

N° 2456 /ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-VUL-P-01\_v1

## PROCEDURE

### VULNERABILTY MANAGEMENT FOR CERTIFIED PRODUCTS

**Application** : As soon as published.

**Diffusion** : Public.

**COURTESY TRANSLATION**



## REVISION HISTORY

Version	Date	Modifications
1	04/03/2026	Creation

In accordance with the April 18<sup>th</sup>, 2002 decree No. 2002-535 as amended, this application note has been submitted to the Executive Certification Committee, who gave a favourable opinion.

It is planned that this application note will be submitted to the Executive Certification Committee for comment when major modifications are made.

This application note is available at the ANSSI's institutional website ([www.cyber.gouv.fr](http://www.cyber.gouv.fr)).

## TABLE OF CONTENTS

1	Subject of the procedure .....	4
2	Context.....	4
3	Procedure for managing vulnerabilities applying to certified product.....	4
3.1	Phase 0 – Preparation for vulnerability management .....	4
3.2	Phase 1 – Receiving and communicating a vulnerability.....	4
3.3	Phase 2 – Impact analysis.....	5
3.4	Phase 3 – Validation of the impact analysis by the certification body.....	6
3.5	Phase 4 – Remediation plan .....	6
3.6	Phase 5 – Validation of the remediation plan by the certification body .....	6
3.7	Phase 6 – New revision release and withdrawal of certificates.....	7
4	Options for the remediation plan.....	7
4.1	Reassessment procedure .....	7
4.1.1	EUCC product.....	7
4.1.2	CSPN product .....	7
4.2	Scope reduction procedure.....	7
4.2.1	EUCC product.....	7
4.2.2	CSPN product .....	7
5	Rating.....	8
6	Processing times .....	8
7	Data protection and retention.....	8
8	Processus overview.....	9
ANNEXE A.	Références .....	10

## 1 Subject of the procedure

This document describes the entire vulnerability management process for a certified product, from detection to the decision to maintain or to withdraw the certificate. It is a specific case of the review of a certificate as defined in [CC-CER-P-01] and [CSPN-CER-P-01]. It specifies the roles of stakeholders in this process (including the certification body, certificate holders, developers, ITSEF and end-users).

This document is based on the vulnerability management guide established as part of the European Common Criteria cybersecurity certification scheme (see [EUCC-Vuln]).

## 2 Context

This procedure applies to all certified products by the national certification center, whose validity date has not expired, and which is impacted by the discovery or publication of a vulnerability calling into question the product's target of evaluation.

## 3 Procedure for managing vulnerabilities applying to certified product

The phases for vulnerability management for a certified product are as follows:

- Phase 0 – Preparation for vulnerability management
- Phase 1 – Receiving and communicating a vulnerability
- Phase 2 – Impact analysis
- Phase 3 – Validation of the impact analysis by the certification body
- Phase 4 – Remediation plan
- Phase 5 – Validation of the remediation plan by the certification body
- Phase 6 – New revision release and withdrawal of certificates

### 3.1 Phase 0 – Preparation for vulnerability management

A certificate holder shall have an organization that allows them to be informed of a potential vulnerability in one of their products.

They may be, for instance, notified of a vulnerability directly by researchers, ITSEF, certification bodies, or any other party.

Furthermore, the certificate holder shall monitor vulnerabilities that could affect their product (see the commitments in the application forms [CSPN-CER-F-01] and [CC-CER-F-01]).

The holder shall be compliant with the requirements described in [ISO/IEC 30111] to define their vulnerability management procedure.

### 3.2 Phase 1 – Receiving and communicating a vulnerability

Upon receipt or identification of a potential vulnerability, a vulnerability impact analysis shall be initiated immediately by the certificate holder.

To determine whether the vulnerability is likely to impact the certificate, the certificate holder, during their analysis, shall ensure that the potential vulnerability:

- can be qualified as “previously undetected”, meaning it is previously unknown,
- concerns the security of the product,

- may have an impact on the compliance with the requirements related to the certification.

If any of the above conditions are not met, the process shall be discontinued and the information identified above shall be recorded in the impact analysis report. This report may be consulted later by the certification body, in particular to verify the certificate holder's analysis.

If the three above conditions are met, the process continues. The certificate holder shall then contact (according to the section "7 Data protection and retention"), within 15 days from the receipt or the identification of the potential vulnerability, the following:

- the certificate holders of products associated with this product ;
- the ANSSI certification body (certification@ssi.gouv.fr) and the CERT (vulnerabilite@ssi.gouv.fr) by:
  - providing the partial impact analysis (with the list of impacted products, their versions, and associated certificates),
  - providing proof that communication has been made to the certificate holders of the products associated with the vulnerability,
  - indicating the date of receipt of the vulnerability and the source of the notification,
  - indicating a code name unrelated to the affected product to designate the vulnerability.

It is recommended to use the [ClubSSI - Regulatory Assistance and Declarations platform](#) to complete this declaration.

The certification body may request further information on the provisions and resources implemented to meet the requirements of this phase.

The certification body will identify that the associated certificates are in the "**monitored**" status (non-public status). This will be notified to the certificate holder with an email.

### 3.3 Phase 2 – Impact analysis

The objective of this phase is to verify the impact of the potential vulnerability on the certificate by updating the previously initiated impact analysis.

The certificate holder will analyze the vulnerability to propose a rating. A description and justification for this rating shall be provided. Based on the rating obtained, the certificate holder will provide a reasoned opinion on the functional resistance and overall resistance of their product.

This analysis may be delegated to a competent trusted third party, for example, an ITSEF, chosen by the certificate holder. The certificate holder shall send their impact analysis report to the certification body with the following information:

- a description of the impacted product(s) and their versions,
- a list of certificates associated with these products and the expiration date of the certificates in question,
- a description of the attack including the type of attack, the impacted mechanism, and the flawed security function,
- the impact of the vulnerability on the certified product,

- any potential risks related to the imminence or availability of an attack,
- if applicable, details on possible exploitation methods for the vulnerability,
- a description of the impact on the target of evaluation,
- the attack rating,
- a conclusion regarding the possible invalidation of the certificate.

The information sent to the certification body shall comply with the certification body's confidentiality rules (see "§7 Data protection and retention") in agreement with the certificate holder.

### 3.4 Phase 3 – Validation of the impact analysis by the certification body

After an internal review (or after discussions with the ITSEF that conducted the assessment), the certification body will be able to:

- validate this impact analysis, or
- reject the analysis.

In the latter case, the certificate holder will resume the procedure from Phase 2 – Impact analysis.

If the attack rating exceeds the resistance identified in the certificate, the process shall be interrupted and the information identified above shall be recorded. The certification body will terminate certificate monitoring.

Otherwise, the vulnerability is confirmed and the certificate is called into question, this one or potentially other ones. In this latter case, the following phases apply for all impacted certificates.

### 3.5 Phase 4 – Remediation plan

If the "Phase 3 – Validation of the impact analysis by the certification body" confirms that the identified vulnerability calls the certificate into question, the certificate holder will submit a remediation plan to manage the vulnerability, incorporating the following options (see §4 Options for the remediation plan):

- reassessment in the event of a product update,
- reduction of the certificate's scope,
- failure to correct the product, requiring withdrawal.

This plan will include a specific schedule of actions to be taken (including the certificate holder's delivery dates, estimated dates for the ITSEF's work, and those of the certification body).

The certificate holder shall without delay notify identified users of the product (including foreign users). This communication will be carried out by the certificate holder's CERTs or incident response teams. Proof of this dissemination of information shall be provided to the certification body. To proceed to the next step, the certificate holder shall transmit this data to the certification body.

### 3.6 Phase 5 – Validation of the remediation plan by the certification body

The remediation strategy shall be validated by the certification body and will be subject to a decision regarding the certificate status. The certificate status may be changed to the public "**suspended**" status according to the rules identified in [CC-CER-P-01]. This information will be communicated to ENISA in case of an EUCC certificate for the purpose of updating their website.

If the certification body rejects the remediation plan, the certificate holder shall propose a new version of this plan (as described in "Phase 4 – Remediation plan").

Rejections may be related to excessively long remediation times, insufficient or incomplete remediation strategies, etc.

### 3.7 Phase 6 – New revision release and withdrawal of certificates

The certificate holder implements their remediation plan in accordance with the previously defined timeline. They will publicly communicate the impact of the vulnerability. The certification body will then withdraw the previous certificates associated with the vulnerable products (the certificate's public status is "**archived**") according to [CC-CER-P-01] or [CSPN-CER-P-01]. The certification body will inform [MCS], which will then report the situation ENISA in case of an EUCC certificate.

In cases where deployment times of new revisions are unusually long, the certificate will be withdrawn by the certification body (the certificate's status is "**archived**").

## 4 Options for the remediation plan

Below are the certificate holder's options for implementing the remediation plan.

### 4.1 Reassessment procedure

#### 4.1.1 EUCC product

The certificate holder shall send to the certification body the form [CC-CER-F-01].

The procedure [CC-CER-P-01] is then applied.

#### 4.1.2 CSPN product

The certificate holder shall send to the certification body the form [CSPN-CER-F-01].

The procedure [CSPN-CER-P-01] is then applied.

### 4.2 Scope reduction procedure

#### 4.2.1 EUCC product

The certificate holder shall send to the certification body the form [CC-CER-F-01], indicating that this is a scope reduction. The note [NOTE-25] defines this mechanism.

The procedure [CC-CER-P-01] is then applied.

#### 4.2.2 CSPN product

A scope reduction cannot be requested under CSPN.

## 5 Rating

Specific rating tables may be defined for certain product categories (see rating tables specific to technical fields identified in [SOTA EUCC]. In other cases, the rating table of [CEM] applies by default.

When [NOTE-18] is applied, its rating table shall be used.

If in doubt regarding the choice of rating table, the certificate holder is invited to contact the national certification center (certification@ssi.gouv.fr).

## 6 Processing times

The deadlines to be met for each phase of this process are defined below:



Regarding Phase 6, in the event of a scope reduction, the maximum deadline for the treatment is 90 days.

In the case of an EUCC certificate, deadlines may be extended after validation of [MCS] by the certification body.

Depending on the criticality of the vulnerability and its exploitation, the above-mentioned nominal deadlines will be reassessed by the certification body.

If these deadlines are not met, certificates will be withdrawn according to [CC-CER-P-01] or [CSPN-CER-P-01].

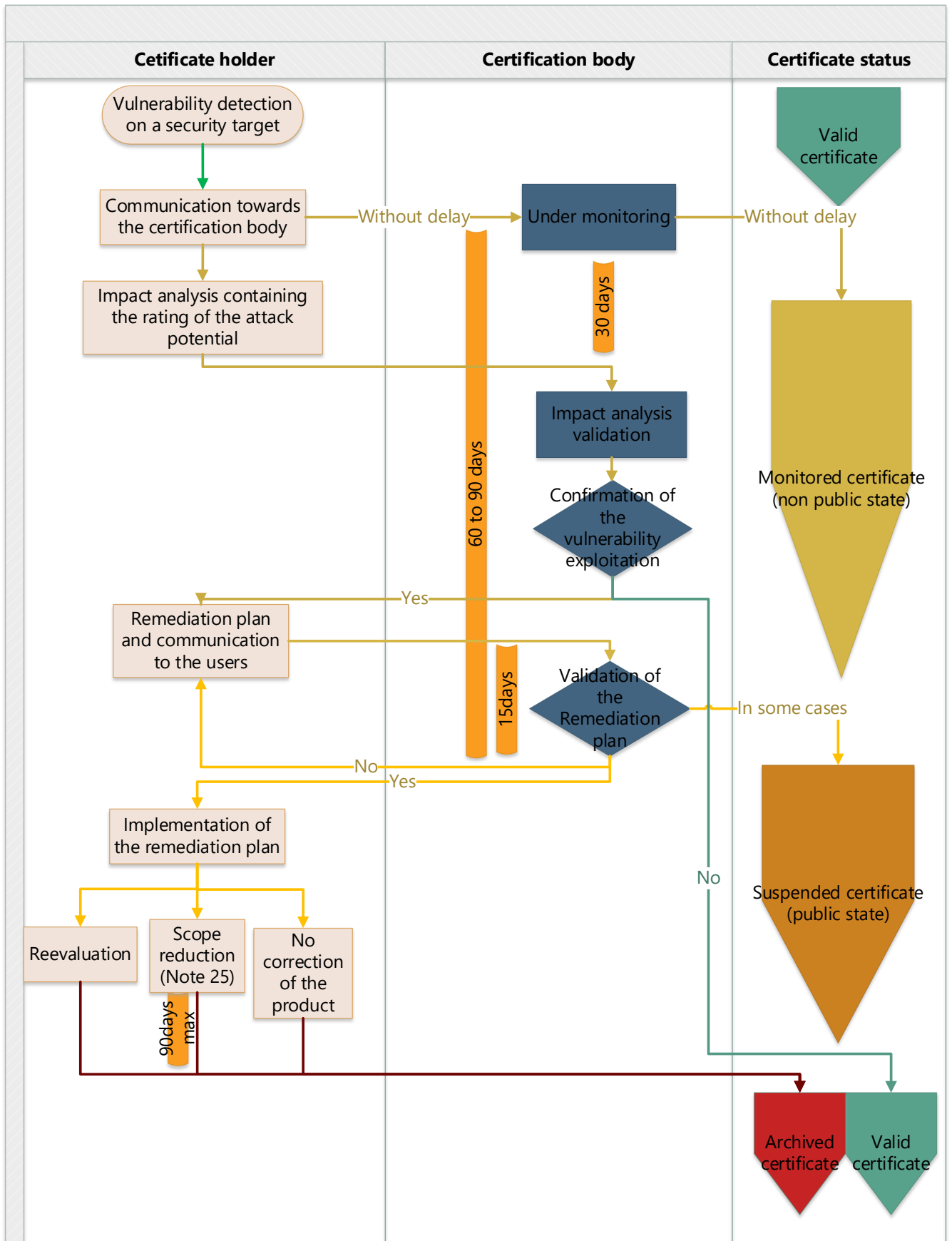
## 7 Data protection and retention

Throughout this procedure, the information exchanged between the various stakeholders shall be encrypted using the following PGP keys:

- CERT-FR (<https://www.cert.ssi.gouv.fr/contact/>),
- Certification body (link : [Comprendre la certification — ANSSI](#))

The certificate holder shall maintain a retention period for this information of at least 5 years for EUCC and 3 years for CSPN; these periods begin on the certificate's expiry date or on the last certificate based on the results of the certificate on which a potential vulnerability was detected (in the case of composition).

### 8 Process overview



## ANNEXE A. Références

Référence	Document
[DECREE]	Decree 2002-535 of the April 18 <sup>th</sup> , 2002, relating to the evaluation and certification of the security offered by information technology products and systems.
[MCS]	Mission contrôles et supervision of ANSSI (corresponding to the National Cybersecurity Certification Authority - NCCA. (ancc@ssi.gouv.fr)
[CC-CER-F-01]	Application form for CC, reference ANSSI-CC-CER-F-01, current version.
[CC-CER-P-01]	CC certification procedure, reference ANSSI-CC-CER-P-01, current version.
[CSPN-CER-F-01]	Application form for CSPN, reference ANSSI-CSPN-CER-F-01, current version.
[CSPN-CER-P-01]	CSPN certification procedure, reference ANSSI-CSPN-CER-P-01, current version.
[NOTE-18]	Tools integration in software assessment, reference ANSSI-CC-NOTE-18, current version.
[NOTE-25]	Scope reduction for a CC certificate, reference ANSSI-CC-NOTE-25, current version.
[ECCG]	European Cybersecurity Certification Group.
[EUCC]	European cybersecurity certification scheme based on common criteria (Implementing Regulation (EU) 2024/482) and its amendments.
[EUCC-Vuln]	Guidelines on vulnerability management and disclosure, Enisa, version 2.1.
[ISO/IEC 30111]	<i>Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité.</i>
[CEM]	<i>Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 18045:2022</i>
[SOTA EUCC]	Application of attack potential to smartcards and similar devices, State of the art documents, Enisa .  Application of attack potential to hardware devices with security boxes, State of the art documents, Enisa.

Most of those documents are available on the ANSSI website ([www.cyber.gouv.fr](http://www.cyber.gouv.fr)).