



**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 24 Février 2026

N° 2417/**ANSSI/SDE/PSS/CCN**

Référence : **ANSSI-CC-VUL-P-01_v1.0**

PROCEDURE

GESTION DES VULNERABILITES DES PRODUITS CERTIFIES

Application : A compter de sa publication.

Diffusion : Publique.

Le sous-directeur « Expertise » de
l'Agence nationale de la sécurité
des systèmes d'information

Renaud LABELLE

[ORIGINAL SIGNE]



SUIVI DES MODIFICATIONS

| Version | Date | Modifications |
|---------|------------|---------------|
| 1.0 | 24/02/2026 | Création |

En application du décret n°2002-535 du 18 avril 2002 modifié, la présente procédure a été soumise, lors de sa création, au comité directeur de la certification, qui a donné un avis favorable.

Cette procédure est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évaluations mineures ne sont pas soumises au comité directeur de la certification.

La présente procédure est disponible en ligne sur le site institutionnel de l'ANSSI (www.cyber.gouv.fr).

TABLE DES MATIERES

| | | |
|-----------|--|----|
| 1 | Objet de la procédure | 4 |
| 2 | Contexte | 4 |
| 3 | Procédure de gestion des vulnérabilités touchant un produit certifié | 4 |
| 3.1 | Phase 0 – Préparation à la gestion des vulnérabilités | 4 |
| 3.2 | Phase 1 – Réception d’une vulnérabilité et communication | 4 |
| 3.3 | Phase 2 – Analyse d’impact | 5 |
| 3.4 | Phase 3 – Validation de l’analyse d’impact par le centre de certification | 6 |
| 3.5 | Phase 4 – Plan de remédiation | 6 |
| 3.6 | Phase 5 – Validation du plan de remédiation par le centre de certification | 7 |
| 3.7 | Phase 6 – Déploiement des nouvelles versions et retrait d’un certificat..... | 7 |
| 4 | Déroulement du plan de remédiation | 8 |
| 4.1 | Procédure de réévaluation | 8 |
| 4.1.1 | Produit EUCC..... | 8 |
| 4.1.2 | Produit CSPN..... | 8 |
| 4.2 | Procédure pour une réduction de portée de certificat | 8 |
| 4.2.1 | Produit EUCC..... | 8 |
| 4.2.2 | Produit CSPN..... | 8 |
| 5 | Cotation | 8 |
| 6 | Délais de traitement | 8 |
| 7 | Protection et conservation des données..... | 9 |
| 8 | Diagramme du processus..... | 10 |
| ANNEXE A. | Références | 11 |

1 Objet de la procédure

Ce document décrit l'ensemble du processus de gestion des vulnérabilités d'un produit certifié de la détection jusqu'à la décision de maintien ou retrait du certificat. Il s'agit d'un cas particulier de réexamen d'un certificat tel que prévu dans [CC-CER-P-01] et [CSPN-CER-P-01]. Il précise le rôle des parties prenantes dans ce processus (cela comprend le centre de certification, les titulaires de certificats, les développeurs, les CESTI et les utilisateurs finaux).

Ce document s'appuie sur le guide de gestion des vulnérabilités établi dans la cadre du schéma européen de certification de cybersécurité fondé sur les critères communs (voir [EUCC-Vuln]).

2 Contexte

Cette procédure s'applique à l'ensemble des produits certifiés par le centre de certification national, dont la date de validité n'est pas échue, et qui sont impactés par la découverte ou la publication d'une vulnérabilité remettant en cause la cible d'évaluation du produit.

3 Procédure de gestion des vulnérabilités touchant un produit certifié

Les phases pour la gestion des vulnérabilités d'un produit certifié sont les suivantes :

- Phase 0 – Préparation à la gestion des vulnérabilités
- Phase 1 – Réception d'une vulnérabilité et communication
- Phase 2 – Analyse d'impact
- Phase 3 – Validation de l'analyse d'impact par le centre de certification
- Phase 4 – Plan de remédiation
- Phase 5 – Validation du plan de remédiation par le centre de certification
- Phase 6 – Déploiement des nouvelles versions et retrait du certificat

3.1 Phase 0 – Préparation à la gestion des vulnérabilités

Le titulaire d'un certificat doit disposer d'une organisation afin d'être informé d'une vulnérabilité potentielle sur l'un de ses produits.

Il peut, par exemple, être notifié d'une vulnérabilité directement par des chercheurs, des CESTI, des organismes de certification ou n'importe quel autre acteur.

Par ailleurs, le titulaire du certificat doit réaliser lui-même une veille sur les vulnérabilités qui pourraient affecter son produit (cf. les engagements présents dans le dossier d'évaluation [CSPN-CER-F-01] et [CC-CER-F-01]).

Le titulaire doit se conformer aux exigences décrites dans [ISO/IEC 30111] pour la définition de sa procédure de gestion des vulnérabilités.

3.2 Phase 1 – Réception d'une vulnérabilité et communication

A partir de la réception ou de l'identification d'une vulnérabilité potentielle, une analyse d'impact de la vulnérabilité doit être lancée sans délai par le titulaire du certificat.

Afin de déterminer si la vulnérabilité est susceptible d'avoir un impact sur le certificat, le titulaire du certificat, durant son analyse, doit analyser si la vulnérabilité potentielle peut :

- être qualifiée de "précédemment non détectée",
- concerner la sécurité du produit,

- avoir un impact sur la cible de sécurité du produit.

Si l'une des conditions ci-dessus n'est pas remplie, le processus est interrompu et les informations identifiées ci-dessus doivent être enregistrées dans le rapport d'analyse d'impact. Celui-ci pourra être consulté ultérieurement par le centre de certification, notamment pour vérifier l'analyse du titulaire du certificat.

Si les trois conditions ci-dessus sont remplies, le processus suit son cours. Le titulaire du certificat doit alors communiquer (conformément au chapitre « 7 Protection et conservation des données ») dans un délai de 15 jours à partir de la réception ou de l'identification de la potentielle vulnérabilité avec :

- Les titulaires de certificats de produits en composition avec ce produit ;
- Le centre de certification (certification@ssi.gouv.fr) ainsi que le CERT (vulnerabilite@ssi.gouv.fr) de l'ANSSI en :
 - fournissant l'analyse d'impact partielle (avec la liste des produits impactés, de leurs versions et des certificats associés),
 - fournissant la preuve qu'une communication a été réalisée auprès des titulaires de certificats de produits en composition,
 - indiquant la date de la réception de la vulnérabilité et la source de notification,
 - indiquant un nom de code sans rapport avec le produit touché pour désigner la vulnérabilité.

Il est recommandé d'utiliser la plateforme [ClubSSI - Assistance et déclarations règlementaires](#) pour réaliser cette déclaration.

Le centre de certification pourra demander la communication des dispositions et des moyens mis en œuvre pour respecter les obligations de cette phase.

Le centre de certification identifiera les certificats associés et les inscrira dans l'état « **surveillé** » (état non public). Il notifiera le titulaire du certificat via un courrier électronique.

3.3 Phase 2 – Analyse d'impact

L'objectif de cette phase est de vérifier l'impact de la vulnérabilité potentielle sur le certificat via la mise à jour de l'analyse d'impact précédemment démarrée.

Le titulaire du certificat devra analyser la vulnérabilité pour proposer une cotation de celle-ci. La description et la justification de cette cotation devra être fournie. En fonction de la cotation obtenue, le titulaire du certificat donnera un avis argumenté sur la résistance des fonctions et la résistance globale de son produit.

Cette analyse pourra être déléguée à un tiers de confiance compétent, par exemple, un CESTI, choisi par le titulaire du certificat.

Le titulaire du certificat devra envoyer son rapport d'analyse d'impact au centre de certification avec les informations suivantes :

- la description du ou des produits impactés ainsi que leurs versions,
- la liste des certificats associés à ces produits ainsi que la fin de date de validité des certificats en question,

- une description de l'attaque incluant le type d'attaque, le mécanisme impacté et la fonction de sécurité défaillante,
- l'incidence de la vulnérabilité sur le produit certifié,
- les risques éventuels liés à l'imminence ou à la disponibilité d'une attaque,
- le cas échéant, des détails sur les moyens d'exploitation possibles de la vulnérabilité,
- la description de l'impact sur la cible d'évaluation,
- la cotation de l'attaque,
- une conclusion sur la remise en question des certificats concernés.

Les informations envoyées au centre de certification devront respecter les règles de confidentialité du centre de certification (cf. « §7 Protection et conservation des données ») en accord avec le titulaire du certificat.

3.4 Phase 3 – Validation de l'analyse d'impact par le centre de certification

Le centre de certification sera en mesure après un examen interne (ou après échanges avec le CESTI qui avait réalisé l'évaluation) de :

- valider cette analyse d'impact, ou
- rejeter l'analyse.

Dans ce dernier cas, le titulaire du certificat reprendra la procédure à partir de la phase « Phase 2 – Analyse d'impact ».

Dans le cas où la cotation de l'attaque est supérieure à la résistance identifiée dans le certificat, le processus est interrompu et les informations identifiées ci-dessus doivent être enregistrées. Le centre de certification met fin à la surveillance du certificat.

Dans le cas contraire, la vulnérabilité est confirmée et remet en cause le certificat ou, le cas échéant, plusieurs certificats. Dans ce cas, les phases suivantes s'appliquent à tous les certificats impactés.

3.5 Phase 4 – Plan de remédiation

S'il est confirmé par la phase « Phase 3 – Validation de l'analyse d'impact par le centre de certification » que la vulnérabilité identifiée remet en cause le certificat, le titulaire du certificat transmettra un plan de remédiation pour remédier la vulnérabilité intégrant les possibilités suivantes (cf. §4 Déroulement du plan de remédiation) :

- Réévaluation en cas de mise à jour du produit,
- Réduction de portée d'un certificat,
- Non correction du produit impliquant un retrait du certificat.

Ce plan comportera un calendrier précis des actions à mener (avec les dates de livraisons du titulaire du certificat, des dates estimatives des travaux du centre d'évaluation et ceux du centre de certification).

Le titulaire du certificat doit prévenir sans délai les utilisateurs identifiés du produit (y compris les utilisateurs étrangers). Cette communication sera réalisée par le CERT ou équipe de réponse à incident du titulaire du certificat. La preuve de cette diffusion d'information devra être fournie au centre de certification.

Le titulaire du certificat, pour passer à l'étape suivante, devra transmettre ces données au centre de certification.

3.6 Phase 5 – Validation du plan de remédiation par le centre de certification

La stratégie de remédiation doit être validée par le centre de certification et fera l'objet d'une décision concernant l'état du certificat. L'état du certificat pourra être passé à l'état public « **suspendu** » selon les règles identifiées dans [CC-CER-P-01].

Dans le cas du refus du plan de remédiation par le centre de certification, le titulaire du certificat doit proposer une nouvelle version de ce plan (comme décrit en phase « Phase 4 – Plan de remédiation »).

Les cas de refus peuvent porter sur des délais de corrections trop longs, des stratégies de remédiations insuffisantes ou non complètes, etc.

3.7 Phase 6 – Déploiement des nouvelles versions et retrait d'un certificat

Le détenteur du certificat applique son plan de remédiation en respectant l'échéancier précédemment défini. Il communique publiquement sur l'impact de la vulnérabilité. Le centre de certification procède ensuite au retrait des certificats associés aux produits vulnérables (état public du certificat « **archivé** ») conformément à [CC-CER-P-01] ou [CSPN-CER-P-01]. Le centre de certification informera de son côté [MCS] qui rapportera la situation à l'ENISA.

Dans les cas où les délais seraient anormalement longs pour le déploiement des nouvelles versions, le centre de certification procède au retrait des certificats associés aux produits vulnérables (état du certificat « **archivé** »).

4 Déroulement du plan de remédiation

Ci-dessous une proposition pour le déroulement du plan de remédiation.

4.1 Procédure de réévaluation

4.1.1 Produit EUCC

Le détenteur du certificat fait une demande au centre de certification via le formulaire [CC-CER-F-01]. La procédure [CC-CER-P-01] s'applique.

4.1.2 Produit CSPN

Le détenteur du certificat fait une demande au centre de certification via le formulaire [CSPN-CER-F-01]. La procédure [CSPN-CER-P-01] s'applique.

4.2 Procédure pour une réduction de portée de certificat

4.2.1 Produit EUCC

Le détenteur du certificat fait une demande au centre de certification via le formulaire [CC-CER-F-01] en indiquant que c'est une réduction de portée. La [NOTE-25] s'applique. La procédure [CC-CER-P-01] s'applique.

4.2.2 Produit CSPN

Une réduction de portée ne peut s'appliquer dans le cadre de la CSPN.

5 Cotation

Des tables de cotation spécifiques peuvent être définies pour certaines catégories de produits (Cf. tables de cotations spécifiques aux domaines techniques identifiées dans les [SOTA EUCC]). Dans les autres cas, la table de cotation de la [CEM] s'applique par défaut.

Lorsque la [NOTE-18] est applicable, elle doit également être prise en compte.

En cas de doute concernant le choix de la table de cotation, le titulaire du certificat est invité à contacter le centre de certification national à certification@ssi.gouv.fr.

6 Délais de traitement

Les délais à respecter pour chaque phase du processus sont définis ci-dessous :



Concernant la Phase 6, en cas de réduction de portée, le délai de traitement maximum est de 90 jours.

Dans le cas de EUCC, les délais peuvent être étendus après validation de [MCS] auprès du centre de certification.

En fonction de la criticité de la vulnérabilité et de son exploitabilité, les délais nominaux ci-dessus seront réévalués par le centre de certification.

Si ces délais ne sont pas respectés, le centre de certification prendra une décision de retrait des certificats associés aux produits vulnérables, conformément à [CC-CER-P-01] ou [CSPN-CER-P-01].

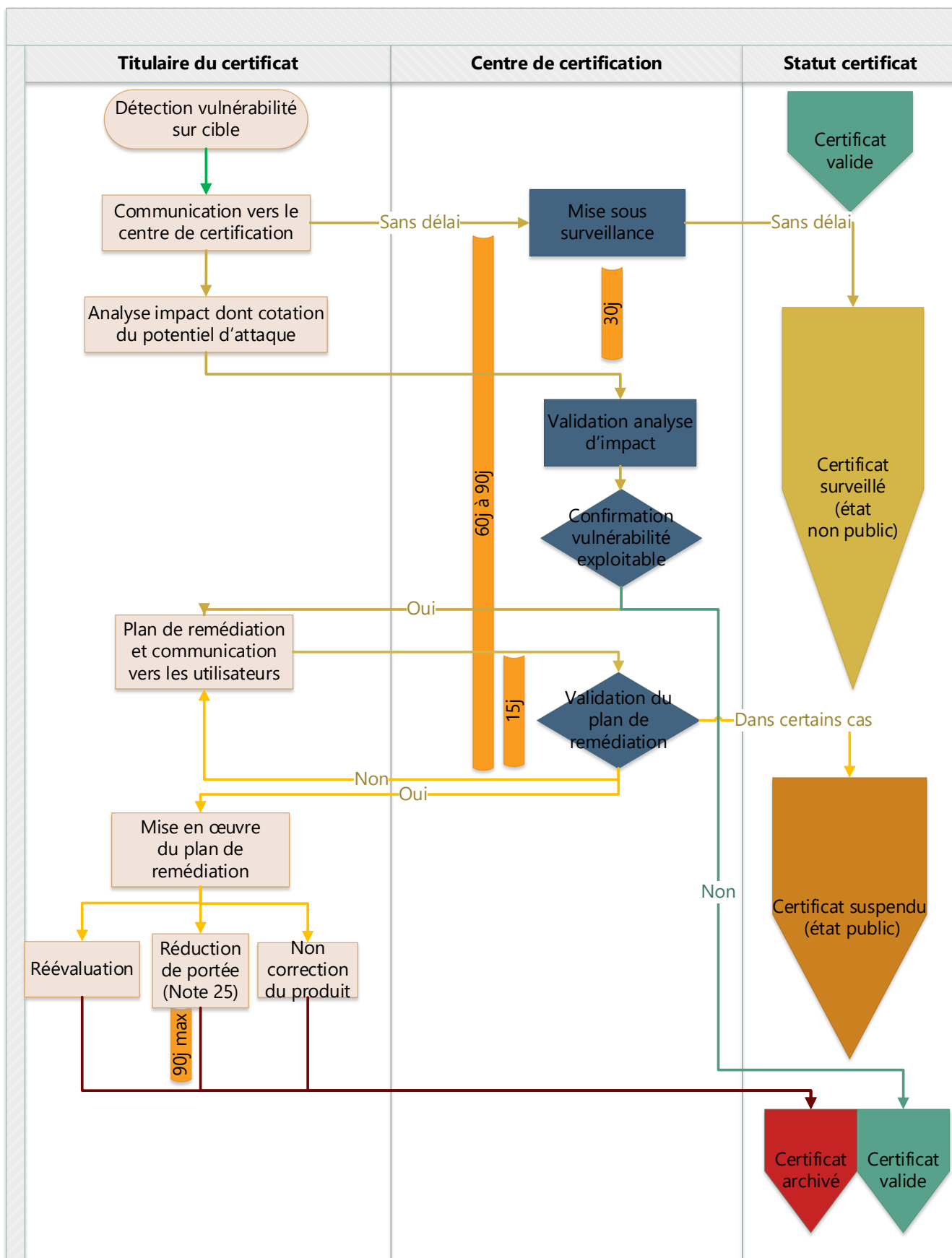
7 Protection et conservation des données

Pour l'ensemble de cette procédure, les informations échangées entre les différentes parties-prenantes doivent être chiffrées en utilisant les clés PGP :

- Correspondances avec le centre de certification CCN : [Comprendre la certification — ANSSI](#),
- Correspondances avec le CERT-FR : <https://www.cert.ssi.gouv.fr/contact/>.

Le titulaire du certificat doit respecter une période de conservation de ces informations a minima de 5 ans pour EUCC et de 3 ans pour CSPN ; ces délais courent à partir de la date de fin de validité du certificat ou du dernier certificat s'appuyant sur les résultats du certificat sur lequel une vulnérabilité potentielle a été détectée (cas de la composition).

8 Diagramme du processus



ANNEXE A. Références

| Référence | Document |
|-----------------|--|
| [DECRET] | Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information |
| [MCS] | Mission contrôles et supervision de l'ANSSI correspondant à l'Autorité Nationale de Certification de Cybersecurité (ancc@ssi.gouv.fr) |
| [CC-CER-F-01] | Dossier d'évaluation en vue d'une certification Critères communs, référence ANSSI-CC-CER-F-01, version en vigueur |
| [CC-CER-P-01] | Certification de cybersécurité fondé sur les critères communs pour les produits et les profils de protection, référence ANSSI-CC-CER-P-01, version en vigueur |
| [CSPN-CER-F-01] | Dossier d'évaluation en vue d'une certification de sécurité de premier niveau (CSPN), référence ANSSI-CSPN-CER-F-01, version en vigueur |
| [CSPN-CER-P-01] | Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version en vigueur |
| [NOTE-18] | Prise en compte des outils dans les évaluations logicielles, référence ANSSI-CC-NOTE-18, version en vigueur |
| [NOTE-25] | Réduction de portée d'un certificat CC, référence ANSSI-CC-NOTE-25, version en vigueur |
| [ECCG] | <i>European Cybersecurity Certification Group</i> |
| [EUCC] | Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements. |
| [EUCC-Vuln] | <i>Guidelines on vulnerability management and disclosure</i> , 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] | <i>Application of attack potential to smartcards and similar devices, State of the art documents</i> , Enisa <i>Application of attack potential to hardware devices with security boxes, State of the art documents</i> , Enisa |

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.cyber.gouv.fr).