CRA SINGLE REPORTING PLATFORM

Fiche d'information relative à la plateforme unique de signalement au titre du règlement sur la cyberrésilience

Comment signaler des incidents et des vulnérabilités activement exploitées sur la plateforme unique de signalement

De quoi s'agit-il?

Depuis le 11 septembre 2026, le règlement sur la cyberrésilience impose aux fabricants de signaler les vulnérabilités activement exploitées et les incidents graves ayant une incidence sur la sécurité des produits comportant des éléments numériques vendus sur le marché de l'UE.

Le règlement sur la cyberrésilience exige également que les intendants de logiciels ouverts signalent ces incidents dans la mesure où ils participent au développement de produits comportant des éléments numériques.

À qui est-ce destiné?

Aux fabricants

Intendants de logiciels ouverts

Quelles sont vos nouvelles obligations de signalement ?

La plateforme unique de signalement au titre du règlement sur la cyberrésilience est un outil en ligne permettant aux fabricants et aux intendants de logiciels ouverts de se conformer à l'obligation de signaler les vulnérabilités activement exploitées et les incidents graves. Conçue pour simplifier les obligations de signalement au sein de l'UE, la plateforme unique de signalement au titre du règlement sur la cyberrésilience est un système électronique permettant d'informer l'ensemble des autorités concernées à partir d'un seul signalement. La plateforme intègre des mesures de sécurité visant à garantir la confidentialité.

Chaque notification permet d'envoyer automatiquement des informations à votre CSIRT national, qui reçoit la notification en premier lieu, aux autres CSIRT nationaux dans lesquels le produit comportant des éléments numériques est disponible, ainsi qu'à l'Agence de l'Union européenne pour la cybersécurité (ENISA).

Comment savoir à quel CSIRT national signaler les incidents ?

En règle générale, le CSIRT national auquel vous devez signaler les incidents sur la plateforme unique de signalement est essentiellement déterminé par votre lieu d'établissement principal. L'article 14, paragraphe 7, du règlement sur la cyberrésilience fournit des informations détaillées qui vous permettront d'identifier le CSIRT national auquel vous devez signaler les incidents.

Quels événements êtes-vous tenu de signaler ?

- **Vulnérabilités activement exploitées :** vulnérabilités présentes dans des produits comportant des éléments numériques, dont on sait qu'elles sont actuellement exploitées par un acteur malveillant, conformément à l'article 3, paragraphe 42, du règlement sur la cyberrésilience.
- **Incidents graves :** incidents ayant une incidence grave sur la sécurité du produit comportant des éléments numériques (par exemple, compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou fonctions), conformément à l'article 3, paragraphe 44; les critères de gravité sont définis à l'article 14, paragraphe 5, du règlement sur la cyberrésilience.

Quand devez-vous signaler de tels incidents ?

La procédure de signalement débute dès que vous prenez connaissance, en qualité de fabricant ou d'intendant de logiciels ouverts, de l'exploitation active d'une vulnérabilité ou d'un incident grave. Il est nécessaire de respecter les délais suivants:

Signalement initial

- dans un délai de **24 heures** à compter de la prise de connaissance de la vulnérabilité ou de l'incident.

Notification de vulnérabilité activement exploitée/d'incident grave

- dans un délai de **72 heures** à compter de la prise de connaissance des faits, en fournissant des informations générales et une première évaluation.

Rapport final:

- **Pour les vulnérabilités :** au plus tard 14 jours après la mise à disposition d'une mesure correctrice (par exemple, un correctif).
- **Pour les incidents graves :** dans un délai d'un mois suivant la notification de vulnérabilité activement exploitée/d'incident grave (elle-même à envoyer dans un délai de 72 heures).

CRA
SINGLE
REPORTING
PLATFORM

Que se passe-t-il une fois les notifications envoyées ?

Une fois les notifications envoyées, le CSIRT qui les a reçues en premier lieu diffuse sans délai ces informations aux autres CSIRT concernés des États membres de l'UE où le produit est également disponible. La notification est mise simultanément à la disposition de l'ENISA.

Les CSIRT nationaux partagent également certaines informations avec leurs autorités de surveillance du marché respectives, afin de leur permettre de s'acquitter de leurs obligations en matière d'application de la réglementation.

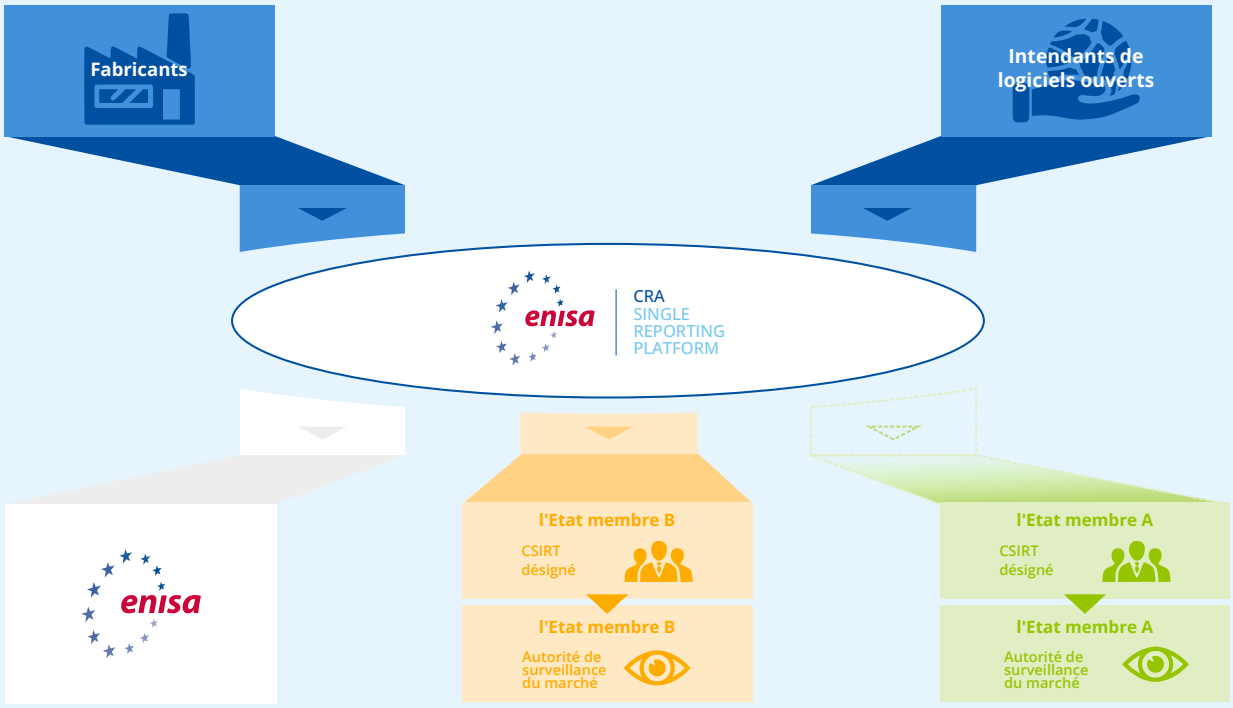
La diffusion de l'information peut-elle être retardée ?

Oui, dans certaines circonstances exceptionnelles, la diffusion de la notification peut être retardée, conformément à l'article 16, paragraphe 2, du règlement sur la cyberrésilience. Le règlement délégué (UE) 2026/881 de la Commission précise les conditions d'application des motifs en ce qui concerne le report de diffusion des notifications.

Comment utiliser la plateforme ?

1. Connexion
2. Sélection du CSIRT national
3. Rédaction du signalement et envoi

Résumé de la procédure de signalement



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Pour obtenir de plus amples informations, veuillez consulter la page de l'ENISA consacrée à la FAQ relative à la plateforme unique de signalement, à l'adresse https://www.enisa.europa.eu/cra-srp, qui comporte également des références aux « lignes directrices de la Commission européenne en lien avec le règlement sur la cyberrésilience », dont la section 9.1 apporte des précisions supplémentaires quant aux obligations de signalement.

Pour toute assistance, veuillez envoyer un message à l'adresse suivante : cra-srp.helpdesk@enisa.europa.eu.