Cybersécurité des produits : la première obligation européenne s'applique dès septembre

Cybersécurité des produits : la première obligation européenne s'applique dès septembre

 Bernard Sfez - 2026-08-11 07:13

Le 11 septembre 2026, le Cyber Resilience Act impose aux fabricants de signaler sous 24 heures toute faille activement exploitée dans leurs produits. Passé ce délai, il reste 72 heures pour la notification complète, puis quatorze jours pour le rapport final. L'obligation ne vise pas seulement les produits à venir : elle vaut pour le parc déjà installé, y compris un équipement livré il y a cinq ans et toujours en service chez un client.

Reste à savoir qui est « fabricant ». Le mot désigne bien plus de monde qu'on ne croit : celui qui vend un plugin ou un module, celui qui assemble un boîtier avec du logiciel embarqué, celui qui distribue une image ou une appliance sous sa marque. À l'inverse, l'hébergeur, l'intégrateur et l'utilisateur final ne le sont pas, et le libre non commercial sort du champ. Voici le test qui permet de trancher, les situations où il s'applique, et ce qu'il reste possible de faire d'ici l'échéance.

Le Cyber Resilience Act, règlement européen 2024/2847 entré en vigueur en décembre 2024, est resté près de deux ans à l'état de sujet de conférence. Le 11 septembre 2026, il devient opposable. Pas dans son intégralité : c'est l'obligation de signalement qui s'active la première, et elle arrive avec des délais que peu d'organisations sont aujourd'hui capables de tenir.

L'échéance est mal comprise pour deux raisons. D'abord parce qu'on la confond avec l'application complète du règlement, prévue en décembre 2027. Ensuite parce que beaucoup pensent que « fabricant de produit numérique » désigne quelqu'un d'autre : un constructeur d'objets connectés, un éditeur de logiciel avec cent salariés. Le règlement ne le voit pas comme ça.

Bonne nouvelle pour ceux qui s'y mettent maintenant : la Commission a approuvé le 27 juillet 2026 ses orientations officielles sur l'application du règlement (document C(2026) 5252). Elles ne sont pas contraignantes, seule la Cour de justice peut trancher, mais les autorités de surveillance s'y référeront. Elles comportent 67 exemples pratiques et une attention explicite aux TPE et PME. C'est le document qui manquait pour répondre aux questions que se posent réellement les petites structures.

Ce qui change le 11 septembre et ce qui ne change pas

Ce qui change :
À partir de cette date, tout fabricant qui a connaissance d'une vulnérabilité activement exploitée dans un de ses produits, ou d'un incident grave affectant sa sécurité, doit émettre une alerte précoce dans les 24 heures. Elle se dépose sur la plateforme unique de signalement gérée par l'ENISA, via le point d'entrée du CSIRT coordinateur de votre pays d'établissement principal, le CERT-FR pour la France. Une notification complète suit sous 72 heures. Puis un rapport final : au plus tard 14 jours après la mise à disposition d'un correctif pour une vulnérabilité, un mois après la notification initiale pour un incident grave.

Vingt-quatre heures, ce sont des heures calendaires. Une faille découverte exploitée un vendredi soir d'août ne vous laisse pas jusqu'au lundi.

Précision utile : « activement exploitée » ne veut pas dire « publiée ». Il faut des éléments fiables établissant qu'un acteur malveillant a exploité la faille sur un système sans autorisation. Une divulgation publique, une preuve de concept ou une démonstration de chercheur ne déclenchent pas, à elles seules, le compte à rebours.

Ce qui ne change pas :
Les exigences de conception, à savoir la sécurité par défaut, la nomenclature logicielle (SBOM), l'absence de vulnérabilité exploitable connue à la mise sur le marché et le marquage CE, n'entrent en jeu qu'en décembre 2027, et seulement pour les produits mis sur le marché après cette date. Votre catalogue existant n'y est pas soumis rétroactivement.

Mais l'obligation de signalement, elle, s'applique au parc existant. Une faille activement exploitée dans un produit que vous avez livré en 2022 doit être signalée sous 24 heures à partir du 11 septembre 2026. C'est la nuance qui piège tout le monde.

Les sanctions pour manquement à cette obligation montent à 15 millions d'euros ou 2,5 % du chiffre d'affaires mondial. Si personne ne s'attend à ce que ce plafond serve contre une TPE, l'obligation, elle, ne dépend pas de votre taille.

Le test en trois questions

Vous êtes fabricant au sens du CRA si vous répondez oui aux deux premières questions, ou à la troisième seule.

1. Fournissez-vous un produit numérique sous votre nom ou votre marque ? Une carte, une sonde, un automate, un boîtier connecté, le firmware qui tourne dedans. Mais aussi un plugin, un thème, un module vendu séparément, une image Docker, une appliance préconfigurée. Ni la taille du produit ni celle de votre entreprise n'entrent en compte. Apposer votre marque sur le produit d'un tiers suffit : vous en devenez le fabricant.

2. Est-ce dans le cadre d'une activité commerciale ? Le logiciel libre développé et distribué hors finalité commerciale est exclu du champ. « Commercial » ne veut pas dire « payant » : un logiciel gratuit dont vous monétisez le support, l'hébergement ou une version pro entre dans le champ.

3. Ou bien : modifiez-vous substantiellement un produit existant avant de le fournir ? Un fork maintenu et redistribué commercialement fait de vous le fabricant du résultat, même sans votre marque dessus.

Sur ce troisième point, les orientations de juillet apportent une précision que tout le monde attendait : une mise à jour de sécurité n'est en principe pas une modification substantielle. Son objet est de réduire le risque. Le critère est l'évolution du profil de risque du produit, pas l'ampleur du changement. Corriger une faille ne vous refait donc pas basculer dans une nouvelle évaluation de conformité.

Si vous avez répondu oui, la suite de cet article vous concerne directement. Et si vous préférez un avis extérieur plutôt que de trancher seul, nous le donnons en une heure.

Situations concrètes

Vous concevez ou assemblez un équipement avec du logiciel embarqué. Sonde, automate, borne, dispositif médical. Vous êtes fabricant sans discussion possible. Et le point qui fait mal : l'obligation vaut pour le parc déjà installé. Un équipement livré en 2021, toujours en service chez un client, dont le firmware embarque une bibliothèque dont la faille est exploitée : signalement sous 24 heures.

Vous vendez un plugin, un thème ou un module. Vous êtes fabricant. C'est le cas le plus fréquemment ignoré.

Vous distribuez une image Docker, une appliance ou une distribution préconfigurée sous votre marque. Vous êtes fabricant, même si tout le contenu est du logiciel tiers. Y compris pour les failles des composants que vous n'avez pas écrits.

Vous portez un projet libre, sans le vendre, mais avec un soutien commercial structuré. Vous relevez probablement du statut de dépositaire de logiciel libre (*open-source software steward*), créé par le règlement pour ce cas précis. Régime allégé : pas de marquage CE, pas d'évaluation de conformité formelle. Mais pas de régime nul. Il faut une politique de cybersécurité écrite, une coopération avec les autorités de surveillance, et, dès le 11 septembre 2026, le signalement des vulnérabilités activement exploitées et des incidents graves affectant les systèmes mis à disposition pour le développement du projet.

Vous revendez ou installez un produit tiers sans y toucher. Vous êtes distributeur, pas fabricant. Le règlement vous donne quand même des devoirs, plus légers : ne pas mettre à disposition un produit dont vous savez qu'il n'est pas conforme, et informer le fabricant ainsi que l'autorité de surveillance si vous découvrez une faille. La vérification du marquage CE viendra s'y ajouter, mais seulement à partir de décembre 2027 : avant cette date, il n'y a rien à vérifier.

Vous installez et maintenez un CMS (Tiki, WordPress), un ERP ou un Nextcloud chez un client. Vous fournissez une prestation, pas un produit mis sur le marché. Vous n'êtes pas fabricant. Vos clients ne le sont pas davantage : ils sont utilisateurs. Même chose pour l'hébergement, l'infogérance et la supervision vendue au mois. Attention toutefois : ce n'est pas parce que le CRA ne s'applique pas qu'aucun régime ne s'applique. Les prestataires de services managés relèvent potentiellement de NIS2, avec ses propres seuils et ses propres obligations. C'est un autre sujet, pas une absence de sujet.

Vous développez du sur-mesure : un thème, un template, une application métier. Les orientations de juillet donnent enfin un critère utilisable, celui de l'endroit où le logiciel s'exécute. Ce qui tourne sur l'appareil de l'utilisateur (application téléchargée, extension de navigateur, client installé localement) est un produit. Une application web utilisée uniquement dans un navigateur, ou un site qui présente de l'information, ne l'est généralement pas, sauf à relever du traitement de données à distance nécessaire au fonctionnement d'un produit. Un thème développé pour un Tiki ou un WordPress consulté au navigateur sort donc du champ. Un plugin distribué et installé chez le client y rentre. Et publier du code source sur un dépôt public ne constitue généralement pas une mise sur le marché.

Si vous êtes fabricant : le minimum avant le 11

Cinq points. Aucun ne demande un budget, tous demandent une décision.

Un canal de signalement public. Une adresse `security@` qui existe vraiment, un fichier `security.txt`, une page de divulgation coordonnée. Sans ça, vous apprendrez l'exploitation de votre faille par un client furieux. Ce n'est pas facultatif : la politique de divulgation coordonnée est une exigence du règlement, écrite, publiée et appliquée.

Savoir qui décide à 2 h du matin. Vous ne pouvez pas vous inscrire à l'avance : l'ANSSI indique que la plateforme unique de signalement ne sera mise en ligne qu'à partir du 11 septembre 2026, l'inscription du fabricant s'y faisant à ce moment-là. Ce qui se prépare en revanche, c'est la décision. Qui décroche, qui a le droit de déclarer, avec quelles informations sous la main.

Une astreinte, même informelle. Le délai de 24 heures ne connaît pas les week-ends.

L'inventaire de vos dépendances. Le SBOM n'est pas exigible avant décembre 2027, mais sans lui

vous ne saurez pas si la CVE du jour vous concerne. Pour un éditeur, un outil d'analyse de composition logicielle produit une première liste en une journée. Pour un fabricant de matériel, c'est un autre chantier : retrouver la chaîne de sous-traitance du firmware, savoir quelle version tourne sur quel lot, et parfois découvrir qu'on n'a aucun moyen de mettre à jour à distance ce qui est déployé. Comptez en mois, pas en après-midi, et commencez maintenant.

De quoi savoir qu'une faille est activement exploitée. Veille CVE, catalogue KEV, alertes CERT-FR, et surtout des journaux et une supervision qui vous montrent une tentative d'exploitation en cours. C'est le point où la plupart des organisations sont aveugles. Une veille CVE adossée à votre inventaire n'est pas un projet à mener une fois, c'est un suivi quotidien. C'est le genre de chose qu'on délègue : nous l'opérons pour nos clients.

Une page de procédure écrite couvre les cinq. Écrivez-la avant septembre.
Le difficile n'est pas de l'écrire, c'est de savoir quoi y mettre. Nous la livrons en cinq jours si vous préférez ne pas partir de zéro.

Un sixième point, à traiter d'ici décembre 2027 mais qui se décide dès maintenant : la période de support. Cinq ans est un plancher, pas une valeur par défaut. Elle doit refléter la durée pendant laquelle le produit est raisonnablement susceptible d'être utilisé, être annoncée au client au moment de l'achat, au moins en mois et année. Si vous vendez du matériel installé pour dix ans, dire cinq ans ne tiendra pas.

Si vous n'êtes pas fabricant : ça vous concerne quand même

L'obligation crée un flux d'information montant. Vos fournisseurs vont devoir déclarer leurs failles exploitées, ce qui rend leur diligence vérifiable, et donc contractualisable.

Quatre points à ajouter à vos contrats et à vos grilles de sélection : le délai sous lequel le fournisseur vous informe (pas l'ENISA, vous) ; la période de support annoncée pour le produit ; l'existence d'un canal de divulgation publié ; la fourniture d'un SBOM à la livraison. Un fournisseur incapable de répondre à ces quatre questions en septembre 2026 vous coûtera cher en décembre 2027.

Ce que ça dit du reste

Le CRA formalise une obligation qui existait déjà en pratique : savoir ce qui tourne chez vous, savoir quand ça casse, savoir qui prévenir. Les organisations qui ont un inventaire, une supervision et une procédure d'incident traiteront le 11 septembre comme une formalité administrative. Les autres découvriront que la conformité n'est pas un document à produire mais une capacité opérationnelle à construire, et que trois semaines n'y suffisent pas.

Si vous lisez ces lignes en août, il vous reste trois week-ends. C'est assez pour écrire une procédure, désigner qui décroche et publier une adresse de contact sécurité. Ce n'est pas assez pour reconstituer la chaîne de sous-traitance d'un firmware livré il y a cinq ans, ni pour équiper d'un mécanisme de mise à jour un parc qui n'en a jamais eu. Faites ce qui tient en une page maintenant, le reste a jusqu'en 2027.

Et si vous hésitez encore sur le côté du test où vous tombez, c'est déjà une réponse : personne ne

devrait découvrir sa qualification réglementaire le jour où la faille est exploitée. La question se règle en une conversation, nos pages sur la conformité CRA donnent le cadre.