CYBER RESILIENCE ACT · ARTICLE 14 · ANNEXE I, PARTIE II

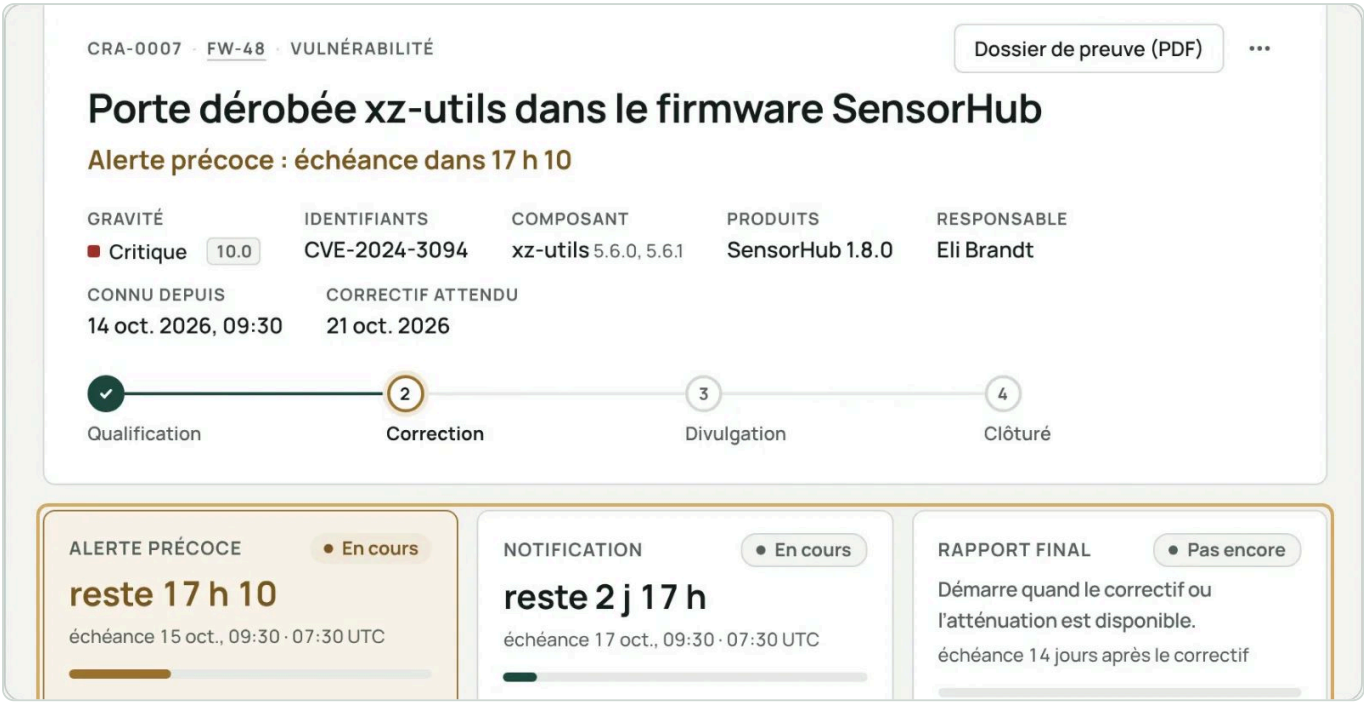
# Une vulnérabilité activement exploitée, signalée depuis Jira

Une vulnérabilité suivie pas à pas, avec des captures de la vraie appli (données de démonstration). Aucune réunion nécessaire : lisez à votre rythme, puis essayez sur votre propre site Jira.

Étape 1

**Trois délais : les deux premiers partent de votre prise de connaissance**

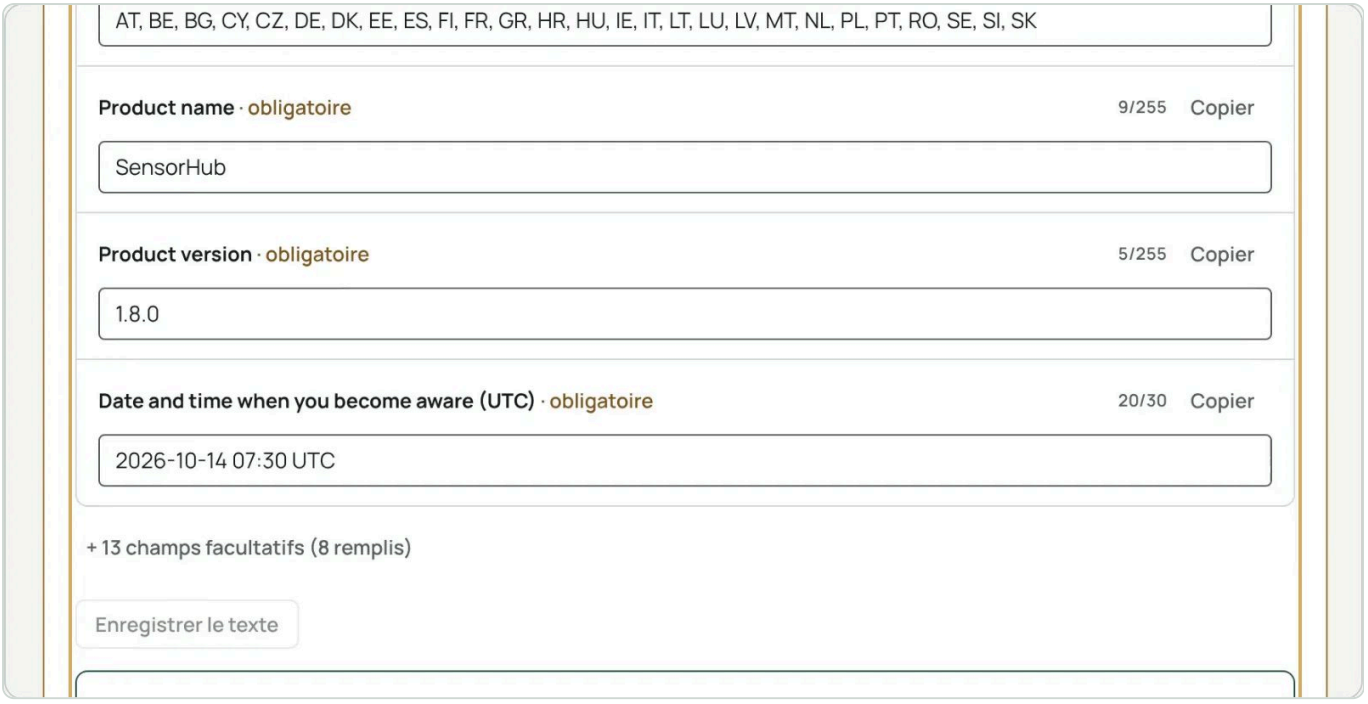
Une qualification signée et datée enregistre si la vulnérabilité est activement exploitée, ou l'incident grave, et quand vous en avez eu connaissance. Dès lors, l'appli décompte l'alerte précoce et la notification. Le rapport final est dû 14 jours après la mise à disposition d'une correction ou d'une atténuation.



Étape 2

### Des champs ENISA prêts à coller

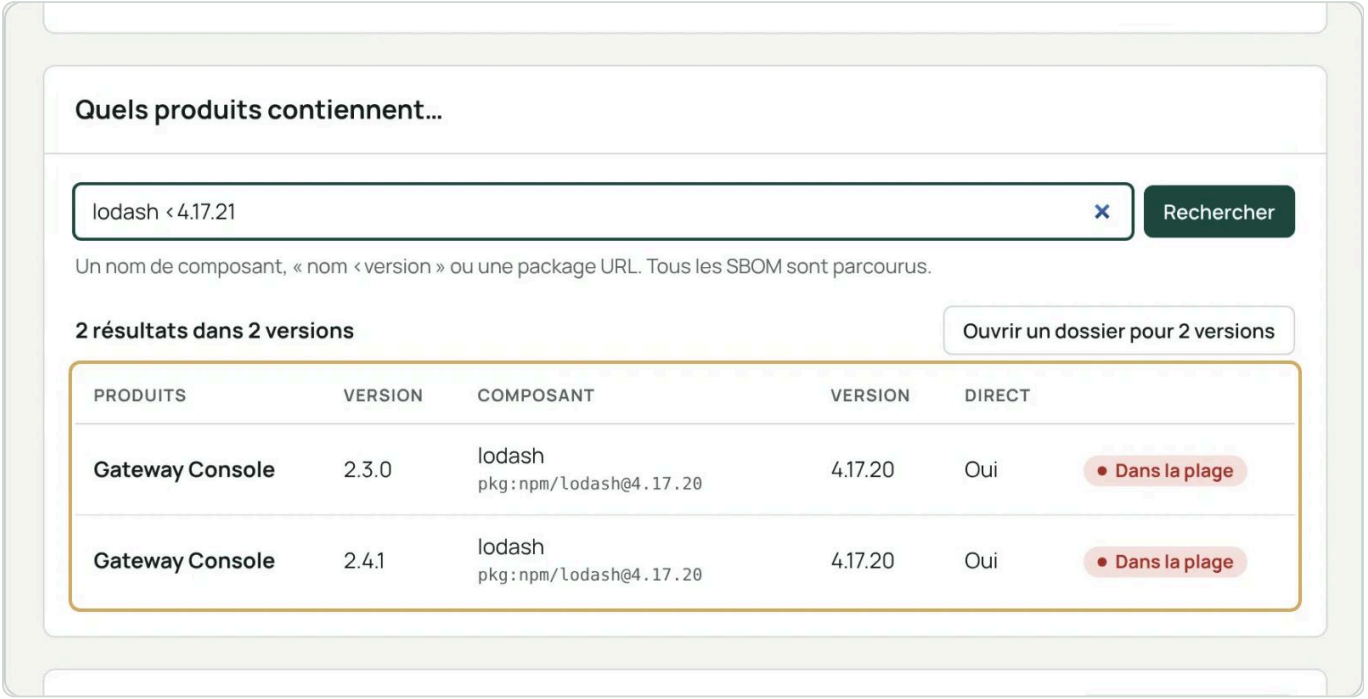
La plateforme unique de signalement de l'ENISA n'offre pas, à ce jour, d'API de soumission. Pour chaque signalement, l'appli prépare chaque champ avec le libellé et la longueur maximale de la plateforme, marque ce qui est obligatoire, et vous laisse les copier un par un ou tous ensemble. Elle n'envoie jamais rien à votre place.




Étape 3

### Quels produits embarquent ce composant ?

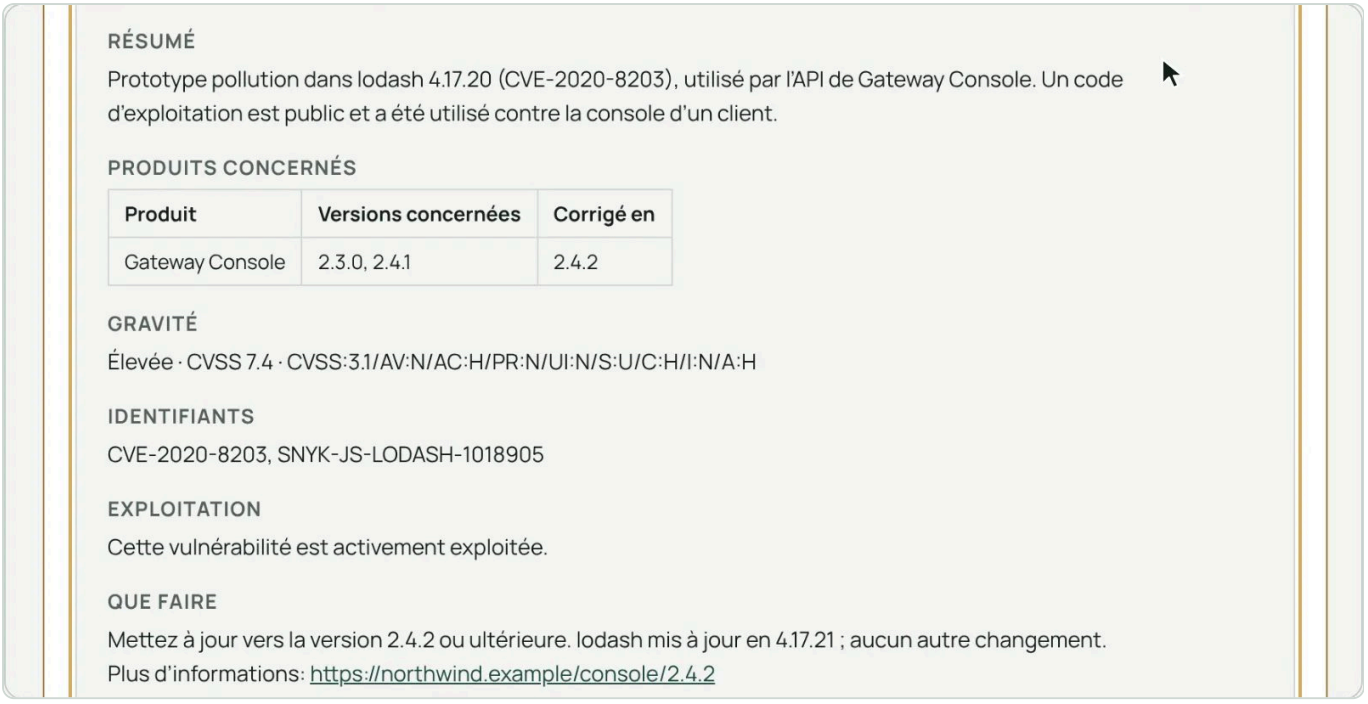
Importez un fichier JSON CycloneDX ou SPDX pour chaque version, puis cherchez un composant ou une URL de paquet : chaque SBOM est parcouru, la plage de versions vérifiée, et un clic ouvre un dossier pour toutes les versions trouvées.



Étape 4

### Correction, utilisateurs informés, avis

Enregistrez la mise à jour de sécurité ou l'atténuation, informez les utilisateurs (article 14, § 8) avec un avis prérempli depuis le dossier, et publiez un avis de sécurité avec un fichier CSAF 2.0 construit depuis l'enregistrement.



RÉSUMÉ

Prototype pollution dans lodash 4.17.20 (CVE-2020-8203), utilisé par l'API de Gateway Console. Un code d'exploitation est public et a été utilisé contre la console d'un client.

PRODUITS CONCERNÉS

| Produit | Versions concernées | Corrigé en |
|---|---|---|
| Gateway Console | 2.3.0, 2.4.1 | 2.4.2 |

GRAVITÉ

Élevée · CVSS 7.4 · CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

IDENTIFIANTS

CVE-2020-8203, SNYK-JS-LODASH-1018905

EXPLOITATION

Cette vulnérabilité est activement exploitée.

QUE FAIRE

Mettez à jour vers la version 2.4.2 ou ultérieure. lodash mis à jour en 4.17.21 ; aucun autre changement.
Plus d'informations: https://northwind.example/console/2.4.2

**Essayez sur votre propre site :** Clearlane CRA a un essai gratuit sur l'Atlassian Marketplace. Vous voulez ce parcours écrit pour votre propre processus ? Écrivez à **maxime@clearlaneapps.com**. Le modèle des 24 premières heures et le dossier fournisseur : **clearlaneapps.com/fr/solutions/cyber**.