Titre :	**Sécurité du code source**		
État :	Approuvé	Effective à partir de :	2022-09-06
		Dernière mise à jour :	2022-09-06

Type :	Orientations		
Code du document :	MSSS-EXI-002	Portée :	MSSS seulement
Mots clés :	Développement; Exigence		
Justification :	La majorité du code source des applications modernes utilise des composants « open-source », souvent dépendantes de d'autres librairies « open-sources », plutôt que du code développé à l'interne. Ces composants peuvent comporter des vulnérabilités qui induisent des risques de sécurité majeurs pour les actifs informationnels. Les outils de type SCA sont les plus efficaces du marché pour détecter les vulnérabilités dans les librairies « open-source ». • Gartner recommande l'utilisation de ce type d'outil et de le considérer lors des premières étapes de mise en œuvre d'un programme de gestion de la sécurité applicative et DevSecOps.		
Lien avec :	• Plan de transformation du MSSS en cybersécurité 2020-2025. • Orientation : MSSS-ORI-002 - Développement sécuritaire. • Présentation « Pilote DevSecOps du MSSS avec Snyk », dans Sharepoint. • Gartner (Décembre 2019), "12 Things to Get Right for Successful DevSecOps" par Neil MacDonald et Dale Gardner. • Forrester (Avril 2021), "Now Tech: Software Composition Analysis, Q2 2021", par Sandy Carielli. • Gartner Research (Février 2022), "Innovation Insight for SBOMs", par Manjunath Bhat, Dale Gardner et Mark Horvath.		

Déclaration :	Gérer les vulnérabilités dans les librairies open-source dans les environnements de développement
Précisions :	
Les vulnérabilités dans les librairies « open-source » doivent être détectées et gérées en fonction de leur niveau de criticité. Pour se faire, un outil d'analyse des vulnérabilités des librairies « open-source » doit être déployé et intégré au processus de développement de chaque actif informationnel (les outils de type SCA–Software Composition Analysis). L'outil doit minimalement produire un rapport identifiant les vulnérabilités des librairies avant chaque mise en production. Les vulnérabilités de niveau CRITIQUE découvertes par l'outil doivent être gérées avant la mise en production de l'actif. Une vulnérabilité est considérée comme gérée dès lors que son correctif a été appliqué, ou encore, que le risque résiduel a été analysé et accepté.	

Déclaration :	Construire la liste des librairies open-source des actifs en Production
Précisions :	
Avant chaque déploiement en production, l'outil d'analyse de vulnérabilité doit construire un inventaire de toutes les librairies « open-source » utilisées par l'actif informationnel. Cet inventaire, appelée « SBOM–Software Bill of Material », permet de conserver l'ensemble des composants « open-source » utilisés en production et leurs dépendances. Cet inventaire permet aux équipes de sécurité du ministère d'évaluer en continu le niveau de sécurité des actifs informationnels, de détecter l'apparition de nouvelles vulnérabilités en production et de réagir rapidement à une menace ou incident de sécurité, le cas échéant.	

Déclaration :	Gérer les vulnérabilités dans les librairies open-source en Production
Précisions :	
Le centre opérationnel de cyberdéfense du ministère (COCD) est responsable de surveiller les composants « open-sources » des inventaires SBOM produits par l'outil d'analyse de vulnérabilités. Des règles d'alertage permettant d'informer le COCD lors de la publication d'une vulnérabilité de niveau CRITIQUE d'un composant « open-source » utilisés dans un actif doivent être mise en œuvre. La stratégie d'alertage doit permettre au COCD d'identifier la portée des actifs informationnels affectés par une vulnérabilité et de réagir rapidement à une menace ou à un incident de sécurité, le cas échéant.	