

GESTION DES VULNÉRABILITÉS ET CORRECTIFS

RÈGLES DE SÉCURITÉ

Référence	FT_SSI-REG-GVC_Gestion des Vulnérabilités et Correctifs_V1.2.docx
Clef GED	263334
Version	V1.2
Classification	Restreint
Date	12/01/2022
État	
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction de la Maîtrise des Risques

Identification du document

Référence	Titre du document	
FT_SSI-REG-GVC_Gestion des Vulnérabilités et Correctifs_V1.2.docx	Gestion des vulnérabilités et correctifs	
Version	État du document	Auteurs
1.2		Filière Sécurité des SI

Classification

Niveau	Diffusion
Restreint	Le personnel de la DSI de France Travail et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité,...)

Mises à jour

Version	Date	Nature de la modification
0.10	25 Novembre 2016	Création dans le cadre de la refonte du référentiel initiée en 2016
0.11	26 Décembre 2016	Maj
1.0	05 janvier 2017	Version finale
1.1	12 janvier 2022	Ajout des éléments liés au SOC
1.2	22 février 2024	Mise à jour suite changement de marque PE → FT

Relectures et validations

Version	Relu par	Direction	Date	Statut
1.0	RSSI Sylvain Lambert	DSI	05/01/2017	validé
1.0	Robert Laupy	DGA-QMR	31/01/2017	validé
1.1	RSSI Sylvain Lambert	DSI	22/02/2022	validé

Documents de référence

Référence	Titre du document
[1] Colibri 196557	Demande de dérogation

SOMMAIRE

1. PRÉAMBULE	5
1.1. Principes fondateurs de la Politique Générale de Sécurité des SI	5
1.2. Enjeux et objectifs du document.....	5
1.3. Champ d'application	5
2. CONCEPTS GÉNÉRAUX	6
2.1. Définition des termes	6
2.2. Cycle de vie d'une vulnérabilité	6
3. RÔLES ET RESPONSABILITÉS.....	7
4. RÈGLES DE SÉCURITÉ.....	8
4.1. Cartographie du SI.....	8
4.2. Gestion des vulnérabilités.....	9
4.3. Gestion des correctifs	10
4.4. Contrôle.....	12
5. ANNEXES.....	13
5.1. Liste des règles.....	13
5.2. Glossaire	14

Règles typographiques

Les termes écrits en vert et soulignés, sont définis dans le glossaire de ce document thématique.

Les règles de la thématique « Gestion des vulnérabilités et correctifs » sont préfixées par le sigle « **GVC-** » et sont numérotées par ordre d'apparition. Elles sont définies dans un encart bleu clair comme figuré ci-dessous :

Définition de la règle

Pour certaines règles, des préconisations, recommandations, commentaires ou des évolutions prévisibles sont détaillés au-dessous de la règle.

Préconisations :

La maîtrise d'œuvre est orientée vers une solution pour couvrir la règle de sécurité.

Recommandations :

L'utilisateur est orienté vers un comportement, un usage, afin de respecter la règle de sécurité.

Commentaires :

Des précisions sont apportées afin d'éclairer la règle énoncée.

1. PRÉAMBULE

1.1. PRINCIPES FONDATEURS DE LA POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SI

Les systèmes d'information hébergent de nombreuses données qui revêtent un caractère stratégique et qui constituent un patrimoine essentiel que France Travail a l'obligation de protéger efficacement.

Pour ce faire, la Direction adopte une Politique Générale de Sécurité des SI qui s'inscrit dans le cadre de la politique de gestion des risques ; cette politique protège les informations et leurs traitements ainsi que les ressources hébergées par les Systèmes d'Information de France Travail.

1.2. ENJEUX ET OBJECTIFS DU DOCUMENT

Un système d'information non mis à jour régulièrement facilite l'exploitation de vulnérabilités. En effet, les codes et autres programmes d'exploitation de failles non corrigées sont régulièrement diffusés publiquement sur les sites internet spécialisés. Il est nécessaire de mettre en œuvre une politique de surveillance et de mise à jour adaptée au système d'information.

La thématique de gestion des vulnérabilités définit les exigences sécurité à mettre en œuvre pour maintenir un niveau de sécurité acceptable face aux risques d'exploitation de vulnérabilités techniques.

Le présent document a pour objectif de définir la procédure de gestion des correctifs de sécurité au sein du système d'information de France Travail.

La gestion des correctifs de sécurité est un processus qui vise à détecter, à analyser et déployer des mises à jour de sécurité.

Le présent document définit les règles de sécurité en matière de gestion des vulnérabilités et correctifs. Ces règles visent à :

- Limiter les risques de compromission du Système d'Information,

1.3. CHAMP D'APPLICATION

Le présent document s'applique sur l'ensemble des ressources informatiques du SI (serveurs, environnements de travail...).

En cas de non-applicabilité d'une des règles du présent document, une procédure de dérogation [1] doit être engagée. Cette demande de dérogation sera transmise au Responsable Sécurité des Systèmes d'Information.

2. CONCEPTS GÉNÉRAUX

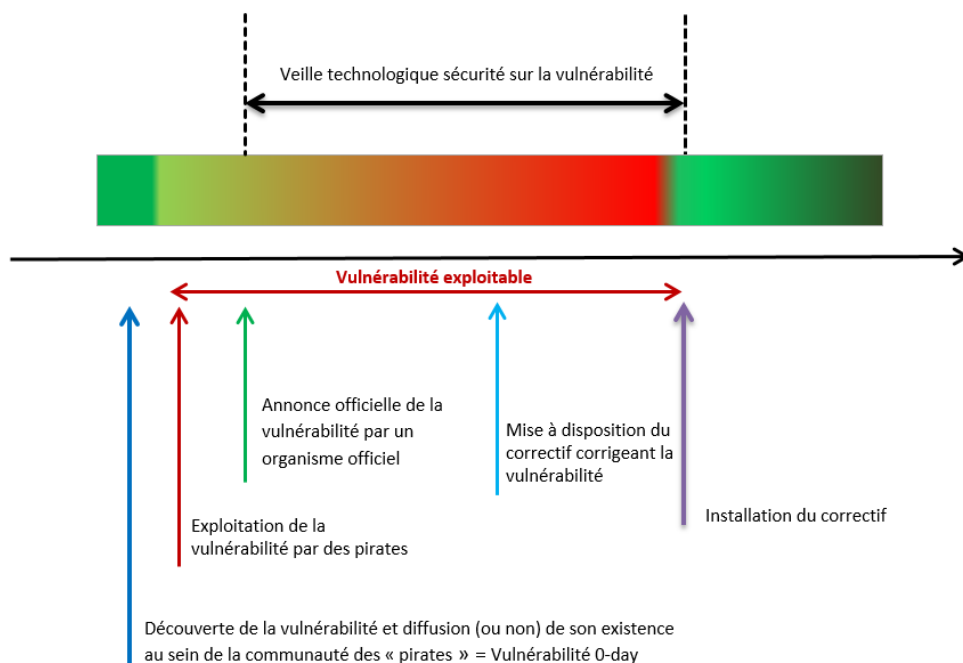
2.1. DÉFINITION DES TERMES

Le terme de correctifs de sécurité couvert par cette Directive doit être, plus précisément, scindé en deux familles de correctifs :

- **Les correctifs de sécurité** au sens littéral : Ensemble de fichiers destinés à corriger ou à améliorer les fonctionnalités sécurité d'un logiciel, que le déploiement soit automatique ou sur initiative.
- **Les correctifs systèmes** : la gestion de ces correctifs a un impact non négligeable sur le niveau de sécurité effective du SI de France Travail. Il est donc nécessaire de les considérer dans cette Directive, même si nous ne les nommons pas autrement que sous l'expression « correctifs de sécurité ».

Les correctifs ne sont pas uniquement destinés à corriger des anomalies existantes, mais servent également à combler des failles qui pourraient être utilisées pour compromettre un système, une application et permettre à un Virus (ou « vers ») de se propager.

2.2. CYCLE DE VIE D'UNE VULNÉRABILITÉ



L'exploitation des vulnérabilités est de plus en plus précoce : une vulnérabilité 0-day, non connue de l'éditeur, peut être exploitée le jour même de sa découverte.

L'installation du correctif permet de mettre fin au risque d'exploitation de la vulnérabilité.

3. RÔLES ET RESPONSABILITÉS

Ce chapitre définit les rôles fonctionnels intervenant dans les processus d'application et de contrôle des règles de sécurité des postes de travail ainsi que les responsabilités associées à chacun de ces rôles :

- Les Métiers
 - ▶ Assurent la classification des informations,
 - ▶ Expriment les besoins de sécurité,
 - ▶ Définissent les exigences de sécurité fonctionnelles.
- La Maîtrise d'Ouvrage Sécurité
 - ▶ Participe à la validation des mesures de sécurité,
 - ▶ Commandite des contrôles de conformité sur leur mise en place.
- La Maîtrise d'Ouvrage Architecture
 - ▶ Traduit les exigences de sécurité en mesures de sécurité,
 - ▶ Définit l'architecture technique,
 - ▶ S'assure de la cohérence entre ce qui est déployé et les exigences de sécurité.
- La Maîtrise d'Œuvre
 - ▶ Met en œuvre et décline les exigences fonctionnelles de sécurité en objectifs et mesures techniques de sécurité adaptées aux infrastructures en place et aux standards internes en vigueur.
- L'Administration et l'Exploitation
 - ▶ Déploient, administrent et maintiennent les infrastructures techniques, dans un état intègre et opérationnel,
 - ▶ Assurent la mise en place des mesures de sécurité,
 - ▶ Maintiennent le niveau de sécurité de leur périmètre de responsabilité...
- Le SOC (Security Operations Center)
 - ▶ Contribue à la veille permanente sur les menaces et les méthodes d'attaques afin de remonter des informations sur les vulnérabilités
 - ▶ Transmet les plans d'action aux entités en charge du traitement des vulnérabilités et apporter un support concernant les correctifs ou palliatifs à mettre en œuvre
 - ▶ Donne un niveau de criticité aux vulnérabilités
 - ▶ Organise la réponse aux incidents de sécurité en assurant la coordination des parties prenantes et en investiguant sur leurs sources.
- Les utilisateurs
 - ▶ Respectent les règles de sécurité sur l'utilisation des systèmes d'information et de communication de France Travail.
 - ▶ Assurent la classification de leurs informations

4. RÈGLES DE SÉCURITÉ

4.1. CARTOGRAPHIE DU SI

GVC- 01 Inventaire du SI

Un inventaire des ressources informatiques du SI doit être établi et maintenu à jour.

Préconisations :

L'inventaire des ressources informatiques peut être constitué de plusieurs référentiels, en fonction des actifs (environnements de travail, serveurs, équipements de sécurité, etc.).

Commentaires :

À titre d'exemple, l'inventaire doit permettre d'obtenir les informations suivantes :

- Le type et la version de l'équipement (serveur physique/virtuel, lame/tour, etc.) ;
- Le type et la version du système d'exploitation ;
- Les applications/middlewares installés ;
- Les mises à jour installées ;

GVC- 02 Criticité des actifs

L'inventaire doit refléter le niveau d'exposition de l'actif :

- Exposition Internet ;
- Exposition Partenaire ;
- Exposition Interne.

GVC- 03 Traitement de l'obsolescence

L'ensemble des actifs doit être supporté par leur éditeur / constructeur. Cela signifie que l'éditeur / constructeur assure un suivi sécurité de son produit, et délivre les correctifs de sécurité lorsqu'une faille est détectée sur son produit.

4.2. GESTION DES VULNÉRABILITÉS

GVC- 04 Veille sécurité

Une veille sécurité doit être effectuée sur l'ensemble des actifs et technologies en place au sein du SI de France Travail, afin d'être informé des vulnérabilités sur les produits, et également lorsqu'un correctif de sécurité est disponible.

Préconisations :

Afin d'identifier au plus tôt les nouvelles menaces, les Responsables de la Sécurité des Systèmes d'information Opérationnel (RSI-Op) doivent entretenir des contacts appropriés avec des associations professionnelles, groupes de spécialistes et des forums spécialisés dans la sécurité de leur environnement opérationnel respectif. Les RSI-Op(s) doivent s'inscrire à des groupes d'intérêt ou des forums spécialisés afin de recevoir à l'avance des alertes, des conseils et des correctifs logiciels concernant les attaques et les vulnérabilités de leur environnement opérationnel respectif.

Le Security Operations Center (SOC) est responsable de mettre en place une veille sur les menaces (threat intelligence), afin prendre en compte l'évolution des types d'attaquants, de leurs motivations, de leurs méthodes d'attaque et de leurs techniques d'attaque.

GVC- 05 Gestion des vulnérabilités critiques

En cas d'une vulnérabilité critique publiée impactant un ou plusieurs composants du SI, celle-ci doit faire l'objet d'une application systématique de la mesure de sécurité, ou de la solution de contournement proposée par l'éditeur ou de la cellule de veille en attendant la publication du correctif de sécurité.

Préconisations :

En attendant le correctif de sécurité, la mesure de sécurité peut-être un arrêt du service / de la fonctionnalité, ou la réalisation d'une action spécifique sur l'application ou sa configuration.

4.3. GESTION DES CORRECTIFS

GVC- 06 Délai d'application des correctifs

Les correctifs de sécurité doivent être appliqués sur les actifs impactés (autres que les environnements de travail), en respectant les délais fixés en fonction du niveau d'exposition de l'actif (cf. description ci-après).

Concernant les actifs de type « Environnement de travail », dès lors que la menace est avérée, les correctifs de sécurité doivent être appliqués sous un délai d'un mois.

Préconisations :

La matrice ci-dessous définit les niveaux d'exposition en fonction de la criticité de la vulnérabilité et le niveau d'exposition de l'actif en dehors des « Environnement de Travail »:

Niveau de criticité de la vulnérabilité	Critique			
	Modérée			
	Faible			
		Interne	Partenaire	Internet

Exposition de l'actif

Légende :

	Niveau d'exposition	Délai d'application des correctifs après publication
	Zone « critique »	Immédiatement dès qu'un exploit est connu
	Zone « majeure »	au prochain <u>WET</u>
	Zone « mineure »	Au prochain <u>WET</u> précédent la SI

GVC- 07 Processus d'application des correctifs

Avant application du correctif en production, ce dernier doit être qualifié et testé afin de s'assurer que le correctif appliqué ait l'effet escompté, et ce, sans effets de bord.

Commentaires :

Le processus d'application des correctifs suit un cycle de mise en production similaire à une évolution applicative :

- Les correctifs sont dans un premier temps installés sur les environnements « fabricants »
- Une fois qu'une période d'observation sans effet de bord a été constatée, la décision de déploiement du correctif en production peut être prise.

GVC- 08 Processus d'application en urgence des correctifs

Un processus d'application en urgence des correctifs doit être défini et implémenté.

Recommandations :

Le processus « Gestion des changements URGENTS en production » doit être utilisé pour l'implémentation des correctifs urgents.

GVC- 09 Tests de non-régression applicative

Lorsque l'application du correctif peut avoir un impact sur les applications, des tests de non-régression applicative doivent être réalisés.

4.4. CONTRÔLE

GVC- 10 Gestion centralisée des correctifs

Le déploiement des correctifs devrait se faire de façon centralisée afin de valider ou non le bon déploiement du correctif, et d'avoir un état des lieux du SI concernant l'application des correctifs.

Préconisations :

La gestion centralisée peut être réalisée sur des outils différents en fonction des technologies

GVC- 11 Scan de vulnérabilités

Des scans de vulnérabilités doivent être effectués régulièrement, et après chaque évolution majeure du SI, sur des ressources dont les services sont exposés sur Internet.

Préconisations :

Le SOC est responsable du paramétrage des outils de scans de vulnérabilité et de la fréquence de ces scans. Il transmet au RSSI ces vulnérabilités remontées par les outils et proposent des mesures correctives ou palliatives lorsque nécessaire.

GVC- 12 Revue des correctifs publiés

Une revue trimestrielle sur les vulnérabilités publiées, évaluées à non-critiques, doit être effectuée pour identifier des correctifs à déployer.

Recommandations :

La consultation du référentiel des vulnérabilités de sécurité maintenu par l'organisme MITRE « <https://cve.mitre.org/> » permettra d'identifier celles dont la version de nos composants est concernée.

GVC- 13 Gestion des ressources non mises à jour

Un inventaire des actifs sur lesquels un ou plusieurs correctifs n'ont pas pu être appliqués doit être défini et maintenu à jour. Cet inventaire doit intégrer les raisons pour lesquelles le correctif n'a pas pu être appliqué, et le plan d'action identifié.

5. ANNEXES

5.1. LISTE DES RÈGLES

GVC- 01	Inventaire du SI.....	8
GVC- 02	Criticité des actifs.....	8
GVC- 03	Traitement de l'obsolescence.....	8
GVC- 04	Veille sécurité	9
GVC- 05	Gestion des vulnérabilités critiques.....	9
GVC- 06	Délai d'application des correctifs	10
GVC- 07	Processus d'application des correctifs	11
GVC- 08	Processus d'application <u>en urgence</u> des correctifs.....	11
GVC- 09	Tests de non-régression applicative.....	11
GVC- 10	Gestion centralisée des correctifs	12
GVC- 11	Scan de vulnérabilités	12
GVC- 12	Revue des correctifs publiés	12
GVC- 13	Gestion des ressources non mises à jour	12

5.2. GLOSSAIRE

DSSI	Département Sécurité des SI
Niveau d'exposition	Le niveau d'exposition d'un actif correspond à son degré d'exposition aux menaces. Trois niveaux existent : ▪ Exposition sur Internet ; ▪ Exposition partenaire ; ▪ Exposition interne.
SOC	Centre Opérationnel de Sécurité (Security Operation Center)
WET	Week-End Technique.