Partagé avec
TLP (Traffic Light Protocol) –
VERT

Approuvé

Norme de la gestion des vulnérabilités

ID du document: **SEC-04**
À l'attention de: Fédération de l'Alliance
Approuvé le 2022-08-24
Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

La compromission due à des vulnérabilités logicielles ou configurationnelles menace la confidentialité, l'intégrité et la disponibilité de l'écosystème et des appareils connectés de la Fédération de l'Alliance de recherche numérique du Canada. La gestion des vulnérabilités est donc une mesure de sécurité destinée à empêcher l'exploitation des vulnérabilités des technologies de l'information qui existent au sein de la Fédération de l'Alliance. En adoptant une approche proactive de la gestion des logiciels présentant des vulnérabilités connues, la Fédération de l'Alliance peut réduire ou éliminer l'exploitation potentielle.

Le but de la présente norme est de définir les exigences pour remédier aux vulnérabilités de l'organisation. Pour ce faire, la norme décrit les rôles concernés, le traitement des systèmes vulnérables, les niveaux de gravité des vulnérabilités et les délais dans lesquels les vulnérabilités de chaque niveau doivent être traitées.

2. Définitions

Reportez-vous à *SEC-00 Glossaire de la sécurité de l'information* pour la définition de termes utilisés dans la présente norme.

- **Vulnérabilité** : Faiblesse dans un système d'information, les procédures de sécurité d'un système, les contrôles internes ou la mise en œuvre qui peut être déclenchée ou exploitée par une source de menace.
- **Gravité** : Mesure dans laquelle une vulnérabilité pourrait avoir un impact sur les systèmes ou les données de la Fédération de l'Alliance.

3. Applicabilité

3.1. La présente norme s'applique à l'infrastructure qui supporte les systèmes et services de la Fédération de l'Alliance.

4 Gestion des vulnérabilités

Les sections suivantes fournissent des conseils et des directives pour chaque étape du cycle de vie de la gestion des vulnérabilités.

4.1 Rôles et responsabilités dans le cycle de vie (matrice « RACI »)

	CCDC* et/ou CCSO**	**CLT*****	**CNS**	**Opérations de sécurité**	**Propriétaire du risque**	**Propriétaire du service**	**Communications (Alliance)**
Maintenir une sensibilisation générale aux vulnérabilités et une posture de sécurité			RC	R		I/R	
Détection des vulnérabilités (4.2.2)			RC	R			
Évaluation de la gravité et des délais requis pour remédier à une vulnérabilité grave (4.2.3)	I	I	RC	C	R	C	C
Évaluation de la gravité et des délais requis pour remédier à une vulnérabilité élevée (4.2.3)		I	RC	C	R	C	C
Évaluation de la gravité et des délais requis pour remédier à une vulnérabilité moyenne (4.2.3)			RC	C	R	C	C
Évaluation de la gravité et des délais requis pour remédier à une vulnérabilité faible (4.2.3)			RC	C	C	R	C
Traitement du système ou du service vulnérable (4.2.4)			I	C	RC	R	
Mesures et rapports (4.2.5)	I		RC	R		C	

*Conseil consultatif et directeur sur la cybersécurité; **Conseil consultatif sur la sécurité opérationnelle;
***Conseil du leadership technologique

Tableau 1 : Matrice RACI – Responsable, Rendeur de compte, Partie consultée, Partie informée

4.2. Cycle de vie

4.2.1 Maintenir une sensibilisation générale aux vulnérabilités et une posture de sécurité

- Le service des Opérations de sécurité doit se tenir au courant des listes de diffusion, des médias sociaux et des autres sources d'information sur la cybersécurité afin de rester au fait des vulnérabilités.
- Les propriétaires de services doivent se prévaloir de diverses sources d'information concernant leurs systèmes et services pour savoir quand les vulnérabilités seront annoncées.
- Les services non utilisés sur les serveurs doivent être désactivés, et les systèmes d'exploitation comme les applications doivent être renforcés contre les menaces externes.
- Les propriétaires de services doivent s'assurer que les actifs de la Fédération de l'Alliance utilisent des versions de logiciels qui sont activement corrigées et renforcées contre les vulnérabilités. Les logiciels en fin de vie ne doivent pas être utilisés.

4.2.2 Détection des vulnérabilités

- Le personnel des Opérations de sécurité se voit confier l'autorité et la responsabilité par rapport à l'analyse des vulnérabilités, selon les dispositions de la présente norme.
- L'analyse automatisée de tous les actifs de la Fédération de l'Alliance sera effectuée au moins une fois par mois, ou manuellement, au cas par cas, lors de la reconnaissance et de la résolution des vulnérabilités graves.
- Toutes les vulnérabilités étiquetées comme étant *moyennes* ou plus dans le *Tableau 2 : Évaluation et traitement* ci-dessous seront traitées conformément à la procédure de réponse aux vulnérabilités.

4.2.3 Évaluation de la gravité et des délais requis pour remédier à une vulnérabilité

- Les scores CVSS (*Common Vulnerability Scoring System*) sont évalués par le MITRE et disponibles dans la *National Vulnerability Database* (NVD) des États-Unis. Obtenez le score de base CVSS pour chaque vulnérabilité et, en tenant compte des mesures de protection et d'atténuation locales, consultez la colonne *Délai cible de traitement* dans le *Tableau 2 : Évaluation et traitement* ci-dessous pour connaître les délais cibles.

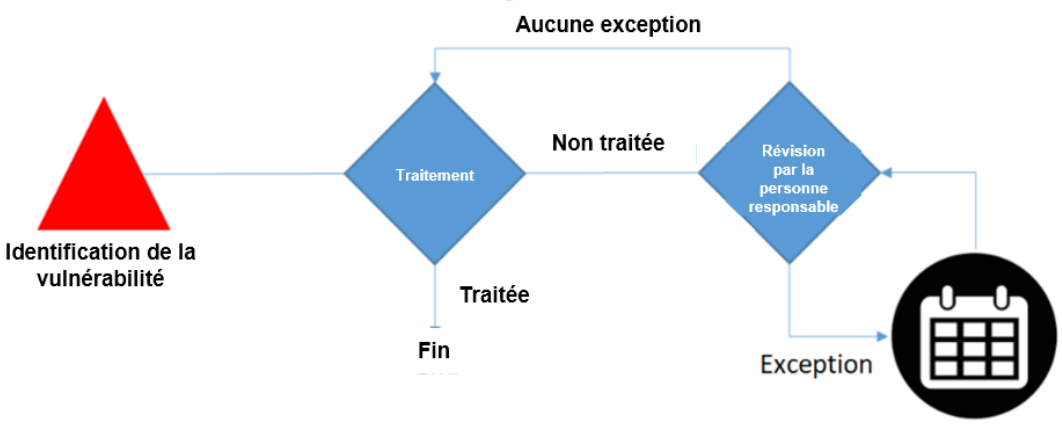
Catégorie	Score	Délai cible de traitement	Parties visées par une exception	Délai cible pour l'exception
	Score de base selon le CVSS[1]	*Délai cible pour l'atténuation initiale et le traitement, une fois disponible*	*La partie responsable est en mesure d'accorder des exceptions aux délais cibles*	*Délai maximum dans lequel les exceptions doivent être examinées et accordées de nouveau*
Grave	9,0–10,0	< 1 jour ouvrable	Propriétaire du risque (doit informer le CCSO et le CLT)	6 mois
Élevé	7,0–8,9	< 10 jours ouvrables	Propriétaire du risque (doit informer le CLT)	12 mois
Moyen	4,0–6,9	< 20 jours ouvrables	Propriétaire du risque	18 mois
Faible	0,1–3,9	Discrétionnaire	Propriétaire du service	24 mois

Tableau 2 : Évaluation et traitement

- Les exceptions aux délais dans la colonne *Délai cible de traitement* doivent être gérées selon le processus illustré et décrit dans la *Figure 1 : Délai cible pour l'atténuation* (ci-dessous) :

[1] Basé sur la dernière version du CVSS au moment de la rédaction des présentes (version 3.1).

Figure 1 : Délai cible pour l'atténuation



- Les parties visées par une exception (mentionnées dans la colonne du tableau 2 ci-dessus) doivent examiner et consigner dans le registre des risques de la Fédération de l'Alliance les vulnérabilités qui peuvent rester non traitées au-delà du temps indiqué dans la colonne *Délai cible de traitement.* Elles doivent également accorder de nouveau toutes les exceptions à l'intérieur de l'intervalle indiqué dans la colonne *Délai cible pour l'exception*.
- Les actifs qui sont sensibles au processus d'analyse doivent être ajoutés au registre des risques et seront exemptés de l'opération si le propriétaire du risque accepte le risque.
- Dans les cas où une vulnérabilité est soupçonnée et qu'un score CVSS n'est pas disponible, les propriétaires de services ou leurs délégués doivent soumettre les détails sur la vulnérabilité au CNS pour examen et analyse, et un accord entre >= 2 membres du CNS sera nécessaire pour déclencher le processus de réponse.
- Dans les cas où une vulnérabilité est susceptible d'avoir un impact sur un nombre important de machines virtuelles installées sur le nuage, un message doit être envoyé aux propriétaires de projets pour les informer de la vulnérabilité et de la manière d'atténuer le risque. L'équipe des communications de la Fédération de l'Alliance sera consultée.
- Pour les vulnérabilités *graves*, le CCSO et le CCDC doivent être informés, en consultation avec l'équipe des communications de la Fédération de l'Alliance.

4.2.4 Traitement du système ou du service vulnérable

- La procédure de réponse aux vulnérabilités doit être suivie pour toutes les vulnérabilités *moyennes* ou supérieures, conformément au *Tableau 2 : Évaluation et traitement*.

- Une fois que les vulnérabilités jugées *élevées* ou *graves* auront été traitées avec succès, le propriétaire du service doit en informer l'équipe des Opérations de sécurité afin que l'actif puisse être réanalysé. Autrement, la prochaine analyse régulière validera le succès du traitement.
- Si une partie responsable soupçonne qu'une vulnérabilité découverte peut être un faux positif, après confirmation avec le personnel des Opérations de sécurité, une diligence raisonnable appropriée sera exercée pour traiter le cas.
- Étant donné que les vulnérabilités peuvent conférer des indices par rapport aux risques et/ou des opportunités d'instaurer de nouveaux contrôles, les propriétaires de services doivent utiliser ces événements pour examiner comment leurs systèmes pourraient être renforcés et quels contrôles pourraient être utilisés pour les protéger contre des vulnérabilités similaires.

4.2.5 Mesures et rapports

- Les mesures, les indicateurs de performance clés et les rapports feront l'objet d'un suivi par l'équipe nationale des Opérations de sécurité, qui en fera rapport au CNS.

5. Information connexe

SEC-00 Glossaire de la sécurité de l'information
Procédure de réponse aux vulnérabilités
Norme de changement, de déploiement et de renforcement des systèmes