Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Évaluation de sécurité du service de notification d'exposition Alerte COVID

PRATICIEN

TLP:WHITE

Canada

AVANT-PROPOS

L'ITSP.10.003, *Évaluation de sécurité du service de notification d'exposition Alerte COVID,* est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité.

Pour de plus amples renseignements sur cette publication, prière de communiquer avec l'équipe du Centre d'appel du Centre pour la cybersécurité :

Centre d'appel
contact@cyber.gc.ca
613-949-7048
1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 14 janvier 2021.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première version.	14 janvier 2021

APERÇU

Le présent document définit la méthodologie et les activités que le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a utilisées pour évaluer la sécurité du service de notification d'exposition Alerte COVID du gouvernement du Canada (GC). L'application mobile Alerte COVID a été lancée le 31 juillet 2020.

En juin 2020, le premier ministre du Canada annonçait que le Canada allait lancer un service de notification d'exposition à la COVID-19 par le biais de Santé Canada. Ce service vise à aider les provinces et les territoires canadiens à identifier et à isoler rapidement la propagation du virus de la COVID-19 tout en assurant un maximum de sécurité et de protection de la vie privée. La mise en œuvre de ce service, plus particulièrement l'application mobile et l'infrastructure de soutien, s'est faite sous la direction du Service numérique canadien (SNC) et a été appuyée par la Division de la cybersécurité du Secrétariat du Conseil du Trésor du Canada (SCT) et le Centre pour la cybersécurité. Afin d'assurer la sécurité et la protection de la vie privée, une approche rigoureuse en matière de sécurité a été adoptée, laquelle privilégie la sécurité système et la protection des renseignements personnels, ainsi que des activités d'évaluation de sécurité. Le SNC et le SCT ont reçu l'appui d'intervenants externes, dont BlackBerry et le Centre pour la cybersécurité, pour effectuer des évaluations et des examens de sécurité indépendants. Le Centre pour la cybersécurité a évalué le service afin d'améliorer sa disponibilité, sa sécurité et son intégrité. L'évaluation a également servi à assurer la sécurité et la protection de la vie privée des Canadiens qui utilisent ce service.

En tant que chargé de projet pour le système, le SCT était responsable de l'exécution des évaluations des risques, de la réalisation de tests fonctionnels et de l'établissement des priorités en matière de modifications de codes sources et de correctifs. Le SNC était également le principal développeur du service, lequel était basé initialement sur le projet code source ouvert COVID Shield conçu par des bénévoles travaillant pour la plateforme Shopify. De plus, le SNC a assuré la mise en œuvre des modifications de codes et des correctifs apportés aux codes sources afin d'atténuer les problèmes.

TABLE DES MATIÈRES

LISTE DES FIGURES

1 INTRODUCTION

La présente publication décrit l'approche et les activités mises en œuvre par le Centre pour la cybersécurité pour réaliser un examen indépendant de l'architecture de sécurité et une évaluation des vulnérabilités du service de notification d'exposition Alerte COVID du GC. Le service est basé sur le cadre développé par Google et Apple, ainsi que le code base source ouvert, COVID Shield.

Le Centre pour la cybersécurité a mis en place une équipe multidisciplinaire formée de chercheurs de vulnérabilités et d'ingénieurs de la sécurité des TI pour évaluer la sécurité du service. Le Centre pour la cybersécurité a évalué le service afin d'améliorer sa disponibilité, sa sécurité et son intégrité. L'évaluation a également servi à assurer la sécurité et la protection de la vie privée des Canadiens qui utilisent ce service. Dans le cadre de l'évaluation, le Centre pour la cybersécurité a identifié les vulnérabilités, a signalé celles-ci au SCT et a formulé des conseils et des recommandations pour l'amélioration de la sécurité globale du service.

L'équipe a utilisé des pratiques exemplaires en sécurité des TI, des pratiques exemplaires en codage, et des conseils publiés par le Centre pour la cybersécurité, comme l'ITSP.40.111 (*Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* [1][1]) et l'ITSG-33 *(La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2]), et le *Mobile Security Testing Guide* de l'organisme Open Web Application Security Project (OWASP) [3].

La section 2 décrit l'analyse de l'architecture de sécurité qu'ont utilisée le Centre pour la cybersécurité et le SCT pour s'assurer que le service respecte les exigences en matière de sécurité et de protection de la vie privée.

La section 3 se consacre à l'évaluation des vulnérabilités, en précisant l'approche de l'équipe du Centre pour la cybersécurité ainsi que les activités de niveau élevé.

[1] Les numéros entre crochets renvoient à du matériel de référence figurant à la section Contenu complémentaire du présent document.

2 ANALYSE DE L'ARCHITECTURE DE SÉCURITÉ

Pour assurer la sécurité du service de notification d'exposition Alerte COVID, l'équipe du Centre pour la cybersécurité a travaillé en collaboration avec des développeurs du SNC et l'autorité opérationnelle de Santé Canada. L'équipe du Centre pour la cybersécurité a évalué la sécurité des composantes suivantes du service :

- l'architecture d'arrière-plan de deux serveurs configurés dans le nuage d'Amazon Web Service (AWS);
- le serveur d'envoi de clés et le serveur de récupération de clés;
- les applications mobiles Android et iOS;
- le portail Alerte COVID.

Le service de notification d'exposition Alerte COVID utilise les portails des provinces pour obtenir les clés de diagnostic. Toutefois, l'équipe ne s'est pas servie de ces portails dans le cadre de l'évaluation.

Il est à noter que BlackBerry a évalué la sécurité du système et du cadre du service, et qu'AWS a utilisé son cadre Well-Architected qui décrit les concepts clés, les principes de conception et les pratiques exemplaires en matière d'architecture pour la conception et l'exécution des charges de travail dans le nuage. Ces évaluations ont été intégrées à l'analyse globale du système.

2.1 APPROCHE D'ÉVALUATION

L'objectif de l'évaluation du Centre pour la cybersécurité était de s'assurer que les contrôles de sécurité mis en place pour le service de notification d'exposition Alerte COVID étaient suffisamment adéquats pour ramener les risques à un niveau acceptable.

L'équipe du Centre pour la cybersécurité a examiné le processus d'évaluation et d'autorisation de sécurité (EAS) du SCT pour le service de notification d'exposition Alerte COVID. Le processus d'EAS, qui est indiqué dans l'ITSG-33 [2], comprend l'établissement de la portée de l'architecture à évaluer, les vulnérabilités et les niveaux de menace identifiés, ainsi que les niveaux de risque connexes. Le Centre pour la cybersécurité a travaillé en collaboration avec le SCT pour obtenir les résultats suivants :

- discuter de l'affectation du risque en fonction des catégories identifiées et fournir de l'assistance en la matière;
- s'assurer que l'inventaire des risques était complet et exact;
- vérifier et caractériser certaines vulnérabilités identifiées;
- passer en revue l'ensemble de l'architecture.

L'équipe du Centre pour la cybersécurité a aussi fait l'analyse de scénarios de menace et a passé en revue l'ensemble de l'architecture du système afin de s'assurer que les contrôles de sécurité appropriés ont été appliqués.

2.2 RÉSULTATS DES ANALYSES

Lors de l'analyse de l'architecture de sécurité, le Centre pour la cybersécurité a constaté que le SCT avait effectué sa propre évaluation de sécurité conformément au processus d'EAS défini dans l'ITSG-33 [2]. Ce processus d'évaluation de sécurité a été effectué de façon minutieuse et approfondie, et il a démontré un haut degré de compréhension du cadre de l'ITSG-33 et de ses processus. Étant donné le court délai accordé et compte tenu du cadre défini, des risques relatifs au service ont été cernés. Toutefois, le SCT a intégré des mesures d'atténuation dans l'architecture du système, ce qui a ramené les risques à un niveau acceptable. Le SCT a travaillé en collaboration avec le Centre pour la cybersécurité pour s'assurer que toutes les vulnérabilités ont été identifiées et atténuées conformément aux niveaux de risque acceptables. L'équipe du Centre pour la cybersécurité a transmis aux décideurs toute l'information disponible sur le risque résiduel (c'est-à-dire le niveau de risque résiduel après la mise en œuvre des contrôles de sécurité) au moment de l'autorisation du système.

3 ÉVALUATION DES VULNÉRABILITÉS

L'équipe du Centre pour la cybersécurité a de plus effectué une évaluation des vulnérabilités du service de notification d'exposition Alerte COVID pour relever les lacunes existantes dans les mesures de protection de la sécurité du service et améliorer la sécurité globale de celui-ci. À la suite de l'évaluation, des vulnérabilités ont été identifiées et signalées au SCT. L'équipe a également émis au SCT des recommandations supplémentaires sur les pratiques exemplaires en sécurité des TI et en codage, présenté des modifications à apporter aux paramètres du système, et validé les bibliothèques cryptographiques.

L'équipe a évalué les aspects suivants du service :

- l'application mobile, les composantes des serveurs de clés et les données connexes;
- le portail Alerte COVID (évaluation limitée);
- les cadres de l'interface de programmation d'applications (API pour *Application Programming Interface*) de notification d'exposition (API de NE) de Google/Apple [4] [5] (évaluation limitée);
- les algorithmes et protocoles cryptographiques;
- les communications d'appareil à serveur et d'appareil à appareil.

Le service utilise des composantes provinciales et propriétaires. Toutefois, ces composantes n'ont pas fait l'objet de l'évaluation du Centre pour la cybersécurité.

Il est à noter que BlackBerry a effectué son propre examen de sécurité du service.

3.1 APPROCHE D'ÉVALUATION

Les tâches liées à l'évaluation ont été réparties en fonction des exigences en matière de sécurité et de la technologie. Les chercheurs ont respecté la vie privée tout au long de leurs activités d'évaluation. Cette évaluation comporte des techniques comme l'analyse du code statique, l'analyse dynamique, les tests à données aléatoires, les tests de pénétration, l'examen d'artefacts judiciaires, l'évaluation des structures de trafic et la vérification de l'authentification du point d'extrémité. Ces techniques sont définies comme suit :

- **Analyse statique – vérification de code de sécurité :** Les chercheurs ont passé en revue le code source d'application et le code source des principales dépendances pour cerner les problèmes potentiels de sécurité, comme des variables non initialisées, des problèmes de gestion de mémoire ou des erreurs de logique.
- **Analyse statistique – rétro-ingénierie :** Les chercheurs ont examiné les artefacts de code machine pour lesquels le code source n'était pas disponible dans le but d'identifier des problèmes potentiels de sécurité.
- **Analyse dynamique** : Les chercheurs ont observé des composantes d'application et interagi avec celles-ci pour identifier des erreurs de logique, des fuites de mémoire et des situations possibles de compétition.
- **Tests à données aléatoires** : Application spécifique d'une analyse dynamique. Les chercheurs ont examiné comment réagissait l'application face à des entrées anormales pour valider la mesure dans laquelle le renforcement de l'application lui permettait de contrer les interactions inattendues.

- **Tests de pénétration :** Réalisation de tests sur un système informatique, un réseau ou une application Web visant à détecter des vulnérabilités que pourrait exploiter un pirate. Les tests de pénétration peuvent inclure toutes les techniques mentionnées ci-dessus.
- **Examen d'artefacts judiciaires :** Enquête axée sur l'examen détaillé des mémoires volatiles et persistantes (comme des systèmes de fichiers) dans le système faisant l'objet du test.
- **Évaluation des structures de trafic :** Examen détaillé des interactions en réseau entre des appareils, et entre un appareil et un serveur.
- **Vérification de l'authentification du point d'extrémité :** Étude des protocoles utilisés par l'application pour authentifier les utilisateurs légitimes d'un serveur et valider les données envoyées par le serveur aux utilisateurs.

3.2 ACTIVITÉS D'ÉVALUATION

Pour effectuer l'évaluation du service, l'équipe a réparti l'application mobile et le serveur de clés en fonction de leurs principales composantes fonctionnelles. Chaque composante a été évaluée individuellement ainsi que dans le cadre d'une solution opérationnelle globale. La figure 1 présente une répartition visuelle du mode d'évaluation utilisé pour l'application, le serveur de clés et le portail Web.

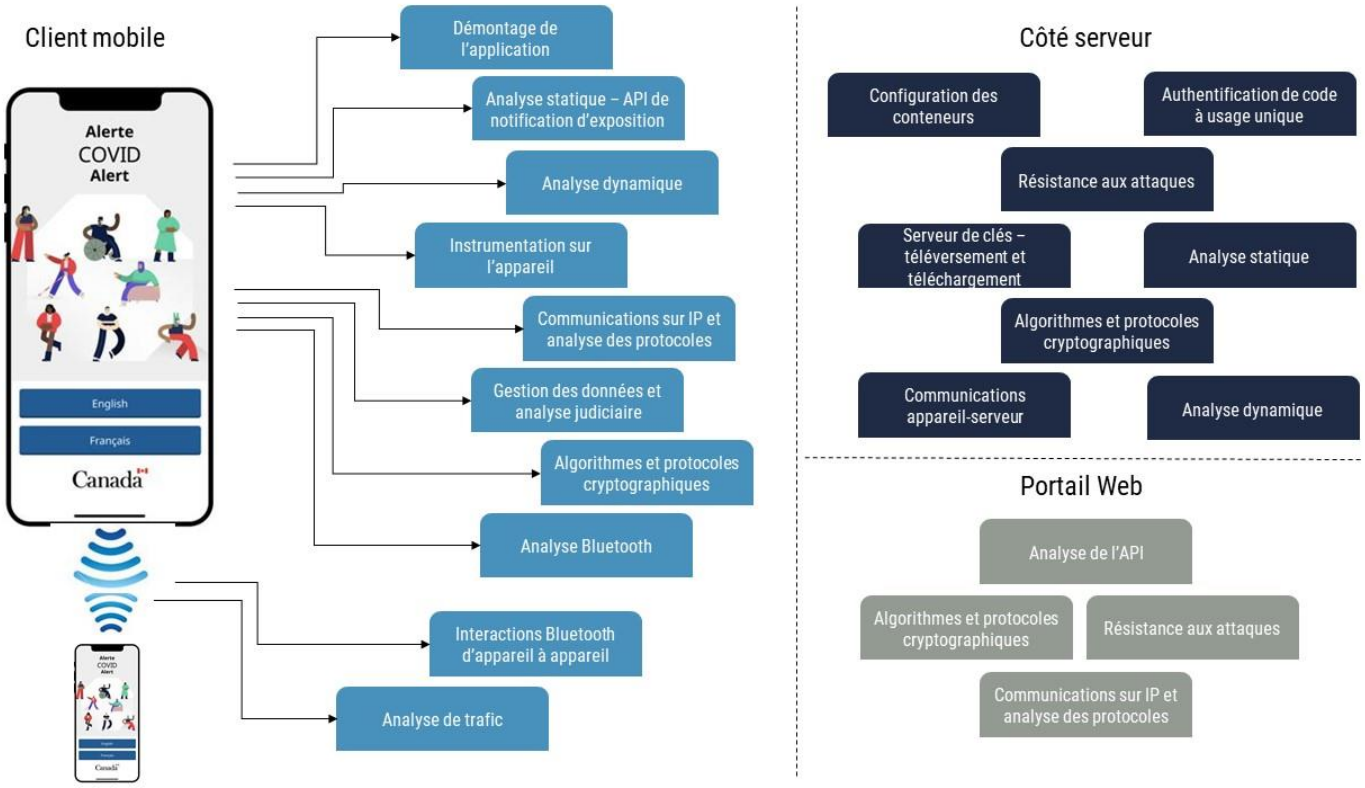

Figure 1 : Répartition des tests d'évaluation des vulnérabilités

Les composantes de l'API de NE mises en œuvre par Google/Apple [4] [5] ont été évaluées sur leurs plateformes respectives.

L'équipe a analysé les composantes cryptographiques mises en œuvre par le service pour en évaluer la sécurité et la puissance cryptographique. Les communications du client mobile vers le serveur de clés et les communications Bluetooth de client mobile à client mobile [6] et le trafic ont été analysés dans les laboratoires du Centre de la sécurité des télécommunications (CST).

L'équipe a de plus réévalué et vérifié les correctifs de sécurité et les modifications de code apportés par le SCT.

3.2.1 APPLICATION MOBILE

Une analyse a également été effectuée sur diverses composantes d'applications mobiles Android et iOS en ayant recours à une combinaison d'analyses statiques et dynamiques. Parmi ces composantes, notons le code source de l'application, la gestion des données et l'instrumentation sur l'appareil, et les protocoles de communications réseau.

ANALYSE STATIQUE DE CODE SOURCE

Une analyse statique a été effectuée sur le code source de l'application mobile, les bibliothèques et les fichiers de configuration connexes disponibles. Le code base comprend plusieurs langages, dont TypeScript, JavaScript, Java, Kotlin, Objective-C et Ruby, ainsi que des bibliothèques partagées précompilées. L'analyse de l'équipe visait principalement à garantir que l'application mobile réponde aux exigences en matière de sécurité et de protection de la vie privée tout en respectant les pratiques exemplaires pour le codage et le développement d'applications.

GESTION DES DONNÉES ET INSTRUMENTATION SUR L'APPAREIL

L'équipe a analysé la façon dont l'application gère les données. Une combinaison des interventions suivantes a été utilisée :

- l'examen de l'endroit où les données d'application sont stockées et de l'utilisation qu'en fait l'application durant son exécution;
- l'examen des artefacts judiciaires pendant la durée de vie de l'application et après sa suppression;
- l'exécution d'une analyse statique;
- la réalisation de tests fonctionnels;
- l'analyse des journaux.

Pour assurer que l'application puisse satisfaire aux exigences en matière de sécurité et de protection de la vie privée, l'analyse comprenait les interventions suivantes :

- vérifier la génération et la protection des identifiants de proximité variable (IPV) et des clés d'exposition temporaire (CET);
- déterminer si l'application tente d'accéder aux données ou de stocker les données auxquelles un accès lui a été donné (p. ex. d'autres renseignements sur l'application, les données de localisation);
- vérifier les paramètres de sécurité par rapport aux lignes directrices sur les pratiques exemplaires;
- vérifier que les données sont générées selon la bonne fréquence;
- déterminer les différences de configuration entre les versions iOS et Android pouvant entraîner des problèmes potentiels de sécurité.

COMMUNICATIONS SUR IP

L'équipe a analysé les protocoles de communications réseau qu'utilise le service et a effectué des tests de pénétration au moyen du cadre de test client-serveur pour générer du trafic sur le réseau. Les principaux objectifs étaient les suivants :

- s'assurer de l'anonymat du client dans les communications;
- vérifier l'authentification des certificats TLS du point d'extrémité;
- déterminer les données qui sont échangées entre l'application et le serveur, et savoir si le trafic sous-jacent peut être sujet à des attaques.

3.2.2 SERVEUR DE CLÉS

Une analyse statique a été effectuée sur le serveur de téléversement et de téléchargement de clés. Bien que tous les types de vulnérabilités aient été pris en considération, l'équipe s'est concentrée sur les questions problématiques comme les situations de compétition et les erreurs de logique au niveau du code source.

Les interactions serveur-base de données et certaines des bibliothèques Go externes qu'utilise le serveur ont été analysées en tenant compte de ce qui suit :

- la manière dont les fournisseurs de soins de santé génèrent un code ponctuel et la gestion du téléversement de clé par le serveur;
- comment le serveur gère les téléversements de clé;
- quelles bibliothèques Go l'application utilise et comment elle les utilise.

L'équipe s'est aussi penchée sur l'environnement dans lequel le serveur est exécuté ainsi que sur l'environnement Docker. Des tests à données aléatoires des points de terminaison du serveur ont également été réalisés pour cerner les failles qui n'auraient pas été décelées lors de l'analyse statique. Pour ce faire, des données arbitraires ont été transmises aux points de terminaison du serveur.

3.2.3 PORTAIL ALERTE COVID

L'analyse statique a été effectuée sur le portail Alerte COVID, qui comporte un code base Django et Python. Tout comme pour le serveur de téléversement et de téléchargement de clés, l'équipe a pris en considération tous les types de vulnérabilités, mais s'est concentrée plus particulièrement sur les questions de logique et les situations de compétition.

3.2.4 API DE NE DE GOOGLE/APPLE

Les cadres d'API de NE de Google/Apple [4] [5] ont été analysés. Au début des examens, le code source de ces composantes n'était pas disponible. L'équipe a donc eu recours à une analyse binaire pour déceler des défauts de base.

Apple et Google ont publié plus tard un code source lié à certaines de ces fonctions, qui a aidé aux examens.

3.2.5 ALGORITHMES ET PROTOCOLES CRYPTOGRAPHIQUES

Plusieurs composantes du service utilisent des algorithmes et des protocoles cryptographiques. L'équipe a évalué ces composantes afin d'assurer que les algorithmes et les protocoles sélectionnés pour la voie de communication entre

l'application et le serveur respectent les conseils publiés par le Centre pour la cybersécurité, comme l'ITSP.40.111 [1] et l'ITSP.40.062 – *Conseils sur la configuration sécurisée des protocoles réseau* [7].

En utilisant les tests tirés de la publication *SP800-90B Recommendation for the Entropy Sources Used for Random Bit Generation* [8] de la National Institute of Standards and Technology (NIST), l'équipe a également évalué la source de l'entropie utilisée pour générer des codes ponctuels pour un diagnostic positif.

3.2.6 COMMUNICATIONS BLUETOOTH/BLUETOOTH À BASSE CONSOMMATION (BLE)

Les communications Bluetooth/BLE (*Bluetooth Low Energy*) [6] ont été analysées à l'aide d'appareils de test dans un environnement isolé dans un laboratoire du CST. Cette démarche s'est déroulée par capture de trafic et analyse de paquets afin de s'assurer que le comportement du Bluetooth répondait aux exigences en matière de sécurité et de protection de la vie privée. L'équipe a particulièrement pris note de la durée de vie des IPV et de la synchronisation des IPV et de la substitution des adresses des appareils Bluetooth.

4 DOCUMENTATION ET PROCESSUS D'ÉLABORATION DE RAPPORTS

Les tâches, les constatations et les mesures d'atténuation proposées ont été documentées à l'aide d'une solution de gestion des problèmes courante. Cette information a été transmise au SCT en temps réel au moyen de tableaux de bord et de mises à jour formelles. Si le SCT décidait de mettre en œuvre une mesure d'atténuation suggérée en fonction de sa propre évaluation des risques et de son classement de risques par priorité, il faisait part de cette décision et de l'état d'avancement des modifications applicables au code en fournissant directement des commentaires.

Les chercheurs ont eu recours à des examens techniques réguliers et à des canaux de discussion pour échanger l'information.

La figure 2 décrit l'analyse et le flux des rapports d'évaluation de haut niveau.

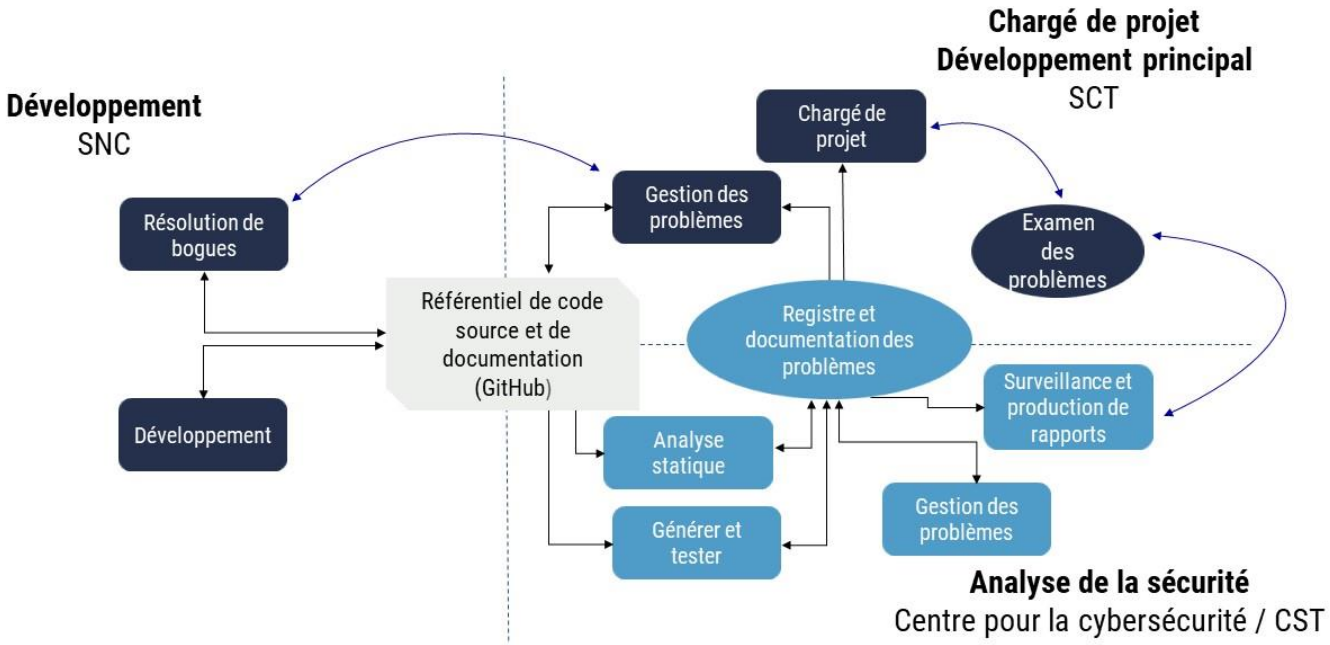

Figure 2 : Analyse et flux des rapports de haut niveau

4.1 PROCESSUS DE GESTION DES PROBLÈMES

Les vulnérabilités et les modifications suggérées en matière de sécurité des TI ont été classées selon les catégories suivantes :

- **Vulnérabilité ou considération en matière de protection de la vie privée** : une réelle vulnérabilité dans le service ou une incidence sur les exigences en matière de protection de la vie privée de l'application;
- **Suggestion** : commentaire sur le style lié à l'examen du code; suggestion sur la façon dont devrait fonctionner le code ou s'il devrait être mis en œuvre autrement.

Les vulnérabilités ont été regroupées selon le niveau de priorité (élevé, moyen ou faible), en fonction de la gravité potentielle. Le SCT a examiné chaque problème soumis et a effectué une analyse des risques afin de déterminer la gravité globale et l'incidence sur le service.

À l'occasion, le Centre pour la cybersécurité a proposé des options d'atténuation aux développeurs du SNC pour qu'ils puissent en prendre connaissance et les analyser. Les développeurs ont réalisé des correctifs de code source et des mises à jour et en ont fait le suivi dans le référentiel GitHub code source ouvert du SNC [9]. Après que le SCT a eu examiné une modification de code et signalé qu'elle était prête à être réévaluée, le chercheur du Centre pour la cybersécurité qui avait initialement évalué et signalé le problème s'est assuré que la mesure d'atténuation a été correctement mise en œuvre. Les chercheurs de vulnérabilités ont également confirmé que la mesure d'atténuation a permis de résoudre le problème sous-jacent sans introduire de nouvelles vulnérabilités. Après la réévaluation et la vérification de la modification, le chercheur devait indiquer que le ticket était terminé.

5 RÉSUMÉ

Dans le but d'appuyer les efforts du SCT visant le service de notification d'exposition Alerte COVID, le Centre pour la cybersécurité a formé une équipe multidisciplinaire de chercheurs de vulnérabilités et d'ingénieurs de la sécurité des TI. L'équipe a évalué l'ensemble de la sécurité du service, a effectué des évaluations des vulnérabilités et a analysé l'architecture de sécurité du service.

Lors de l'analyse de l'architecture de sécurité, le Centre pour la cybersécurité a constaté que le SCT avait effectué son évaluation de sécurité conformément au processus d'EAS défini dans l'ITSG-33 [2]. Le processus d'évaluation de sécurité du SCT a été effectué de façon minutieuse et approfondie, et il a démontré un haut degré de compréhension du cadre ITSG-33 [2] et de son processus. Le SCT a travaillé en collaboration avec le Centre pour la cybersécurité pour s'assurer que toutes les vulnérabilités ont été identifiées et atténuées conformément aux niveaux acceptables de risque.

À la suite de l'évaluation du Centre pour la cybersécurité, plusieurs vulnérabilités ont été identifiées et signalées au SCT. L'équipe a également émis au SCT des recommandations supplémentaires sur les pratiques exemplaires en sécurité des TI et en codage, présenté des modifications à apporter aux paramètres du système, et validé les bibliothèques cryptographiques.

L'évaluation a permis de démontrer un degré élevé de confiance quant au processus et aux résultats obtenus, confirmant ainsi que le système est sécuritaire. Le risque résiduel a été identifié et caractérisé pour les décideurs au moment de l'autorisation du système. Le SCT continue ses efforts afin de trouver et d'atténuer les risques pendant le fonctionnement du système.

5.1 COORDONNÉES

Pour obtenir de plus amples renseignements, prière de communiquer avec l'équipe du Centre d'appel du Centre pour la cybersécurité par courriel ou par téléphone :

Centre d'appel
contact@cyber.gc.ca
613-949-7048
1-833-CYBER-88

6 CONTENU COMPLÉMENTAIRE

6.1 LISTE DES ABRÉVIATIONS

Terme	Définition
API de NE	Interface de programmation d'application (API pour *Application Programming Interface*) de notification d'exposition
AWS	Amazon Web Services
BLE	Bluetooth à basse consommation (*Bluetooth Low Energy*)
CET	Clé d'exposition temporaire
CST	Centre de la sécurité des télécommunications
GC	Gouvernement du Canada
IPV	Identifiant de proximité variable
NIST	National Institute of Standards and Technology
SCT	Secrétariat du Conseil du Trésor du Canada
SNC	Service numérique canadien
TI	Technologies de l'information
TLS	Sécurité de la couche de transport (*Transport Layer Security*)

6.2 GLOSSAIRE

Terme	Définition
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril sa confidentialité, son intégrité ou sa disponibilité.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des politiques, des pratiques et des procédures de sécurité.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, logiciels, et matériels (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés ou les compromissions.
Évaluation des vulnérabilités	Processus visant à déterminer les faiblesses ou les lacunes existantes dans le cadre des efforts de protection d'un système d'information.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. L'intégrité s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel ainsi qu'au personnel.
Protégé B	Désignation de sécurité du gouvernement fédéral qui s'applique aux renseignements ou aux biens dont la compromission pourrait porter un préjudice grave à une personne, à une organisation ou à un gouvernement.
Risque	Degré de probabilité qu'une menace exploite une vulnérabilité pour accéder à un bien et répercussions connexes. Habituellement le risque est exprimé en fonction d'un niveau (faible, moyen ou élevé).
Risque résiduel	Degré de probabilité et répercussions potentielles d'une menace qui subsistent après la mise en application des contrôles de sécurité.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens ou les activités d'une organisation.

6.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)*, août 2016.
2	Centre canadien pour la cybersécurité, *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
3	Open Web Application Security Project Foundation, *OWASP Mobile Security Testing Guide*, sans date.
4	Apple, *Exposure Notification API Framework,* sans date.
5	Google Inc., *Google Exposure Notification API*.
6	Bluetooth SIG Inc., Bluetooth Specifications.
7	Centre canadien pour la cybersécurité, *ITSP.40.062 – Conseils sur la configuration sécurisée des protocoles réseau*, version 2, octobre 2020.
8	National Institute for Standards and Technology, *SP800-90B Recommendation for the Entropy Sources Used for Random Bit Generation*, janvier 2018.
9	Service numérique canadien et GitHub, Canadian Digital Service GitHub Repository, sans date.
10	Electronic Frontier Foundation (EFF), *Apple and Google's COVID-19 Exposure Notification API: Questions and Answers*, avril 2020.
11	National Institute of Standards and Technology, Cryptographic Algorithm Validation Program.
12	National Institute of Standards and Technology, Cryptographic Module Validation Program.
13	Ministère de la Santé et ministère de l'Innovation technologique de l'Italie et GitHub, *Immuni's Traffic Analysis Mitigation*, sans date.
14	National Cyber Security Centre (Royaume-Uni), *NHS Test and Trace App Security Redux*, août 2020.
15	National Institute of Standards and Technology, *SP 800-115 Technical Guide to Information Security Testing and Assessment*, septembre 2008.
16	Commissariat à la protection de la vie privée du Canada, *La Loi sur la protection des renseignements personnels*.